kaspersky

Kaspersky Embedded Systems Security

© 2020 АО «Лаборатория Касперского».

Содержание

О Kaspersky Embedded Systems Security

Что нового

Источники информации о Kaspersky Embedded Systems Security

- Источники для самостоятельного поиска информации
- Обсуждение программ "Лаборатории Касперского" в сообществе пользователей

Kaspersky Embedded Systems Security

- Комплект поставки
- Аппаратные и программные требования
- Функциональные требования и ограничения
  - Установка и удаление
  - Мониторинг файловых операций
  - Управление сетевым экраном

Установка и удаление программы

- Коды программных компонентов Kaspersky Embedded Systems Security для службы установщика Windows
  - Программные компоненты Kaspersky Embedded Systems Security
  - Программные компоненты набора Средства администрирования
- Изменения в системе после установки Kaspersky Embedded Systems Security
- Процессы Kaspersky Embedded Systems Security
- Параметры установки и удаления и ключи командной строки для службы установщика Windows
- Журналы установки и удаления Kaspersky Embedded Systems Security
- Планирование установки
  - Выбор средств администрирования
  - Выбор способа установки
- Установка и удаление программы с помощью мастера
  - Установка с помощью мастера установки
    - Установка Kaspersky Embedded Systems Security
    - Установка Консоли Kaspersky Embedded Systems Security
    - Дополнительная настройка после установки Консоли программы на другое устройство
      - Разрешение анонимного удаленного доступа к программам COM
      - Разрешение сетевых соединений для процесса удаленного управления Kaspersky Embedded Systems Security
      - Добавление правила исходящего подключения для брандмауэра Windows
    - Действия после установки Kaspersky Embedded Systems Security
      - Запуск и настройка задачи Обновление баз программы
      - Проверка важных областей
  - Изменение состава компонентов и восстановление Kaspersky Embedded Systems Security
  - Удаление с помощью мастера установки
    - Удаление Kaspersky Embedded Systems Security
    - Удаление Консоли Kaspersky Embedded Systems Security
- Установка и удаление программы из командной строки
  - Об установке и удалении Kaspersky Embedded Systems Security из командной строки
  - Примеры команд установки Kaspersky Embedded Systems Security
  - Действия после установки Kaspersky Embedded Systems Security
  - Добавление и удаление компонентов. Примеры команд
  - Удаление Kaspersky Embedded Systems Security. Примеры команд
  - Коды возврата
- Установка и удаление программы с помощью Kaspersky Security Center

Общие сведения об установке через Kaspersky Security Center
Права для установки или удаления Kaspersky Embedded Systems Security
Установка Kaspersky Embedded Systems Security с помощью Kaspersky Security Center
Действия после установки Kaspersky Embedded Systems Security
Установка Консоли программы через Kaspersky Security Center
Удаление Kaspersky Embedded Systems Security с помощью Kaspersky Security Center
Установка и удаление программы через групповые политики Active Directory
Установка Kaspersky Embedded Systems Security через групповые политики Active Directory
Действия после установки Kaspersky Embedded Systems Security
Удаление Kaspersky Embedded Systems Security через групповые политики Active Directory
Проверка функций Kaspersky Embedded Systems Security. Использование тестового вируса EICAR
О тестовом вирусе EICAR
Проверка функций постоянной защиты файлов и проверки по требованию
Прочие ограничения
Интерфейс программы
Лицензирование программы
О Лицензионном соглашении
О лицензии
О Лицензионном сертификате
О ключе
О файле ключа
О коде активации
О предоставлении данных
Активация программы с помощью файла ключа
Активация программы с помощью кода активации
Просмотр информации о действующей лицензии
Функциональные ограничения после окончания срока действия лицензии
Продление срока действия лицензии
Удаление ключа
Работа с Плагином управления
Управление Kaspersky Embedded Systems Security из Kaspersky Security Center
Управление параметрами программы
Навигация
Переход к общим параметрам из политики
Переход к общим параметрам из окна свойств программы
Настройка общих параметров программы в Kaspersky Security Center
Настройка масштабируемости и интерфейса в Kaspersky Security Center
Настройка параметров безопасности в Kaspersky Security Center
Настройка параметров соединения в Kaspersky Security Center
Настройка запуска по расписанию локальных системных задач
Настройка параметров карантина и резервного хранилища в Kaspersky Security Center
Создание и настройка политик
Создание политики
Разделы параметров политики Kaspersky Embedded Systems Security
Настройка политики
Создание и настройка задач в Kaspersky Security Center
О создании задач в Kaspersky Security Center
Создание задачи в Kaspersky Security Center

- Настройка локальных задач в окне Параметры программы в Kaspersky Security Center
- Настройка групповых задач в Kaspersky Security Center
  - Задача Активация программы
  - Задачи обновления
  - Проверка целостности программы
- Настройка параметров диагностики сбоев в Kaspersky Security Center
- Работа с расписанием задач
  - Настройка расписания запуска задач
  - Включение и выключение запуска задач по расписанию
- Отчеты в Kaspersky Security Center

Работа с Консолью Kaspersky Embedded Systems Security

- О Консоли Kaspersky Embedded Systems Security
- Интерфейс Консоли Kaspersky Embedded Systems Security
  - Окно консоли Kaspersky Embedded Systems Security
  - Значок области уведомлений в панели задач
- Управление Kaspersky Embedded Systems Security через Консоль программы, установленную на другом устройстве
- Настройка общих параметров программы в Консоли программы
- Управление задачами Kaspersky Embedded Systems Security
  - Категории задач Kaspersky Embedded Systems Security
  - Запуск / приостановка / возобновление / остановка задачи вручную
  - Работа с расписанием задач
    - Настройка расписания запуска задач
    - Включение и выключение запуска задач по расписанию
  - Использование учетных записей для запуска задач
    - Об использовании учетных записей для запуска задач
    - Указание учетной записи для запуска задачи
  - Импорт и экспорт параметров
    - Об импорте и экспорте параметров
    - Экспорт параметров
    - Импорт параметров
  - Использование шаблонов параметров безопасности
    - О шаблонах параметров безопасности
    - Создание шаблона параметров безопасности
    - Просмотр параметров безопасности в шаблоне
    - Применение шаблона параметров безопасности
    - Удаление шаблона параметров безопасности
- Просмотр состояния защиты и информации о Kaspersky Embedded Systems Security

Работа с Веб-плагином

- Управление Kaspersky Embedded Systems Security из Kaspersky Security Center Web Console
- Ограничения Веб-плагина
- Управление параметрами программы
  - Настройка общих параметров программы в Kaspersky Security Center Web Console
    - Настройка масштабируемости и интерфейса в Kaspersky Security Center Web Console
    - Настройка параметров безопасности в Kaspersky Security Center Web Console
    - Настройка параметров соединения в Kaspersky Security Center Web Console
    - Настройка запуска по расписанию локальных системных задач
  - Настройка параметров карантина и резервного хранилища с помощью Веб-плагина
- Создание и настройка политик

Создание политики
Разделы параметров политики Kaspersky Embedded Systems Security
Создание и настройка задач в Kaspersky Security Center
О создании задач в Kaspersky Security Center Web Console
Создание задачи в Kaspersky Security Center Web Console
Настройка групповых задач в Kaspersky Security Center
Настройка параметров диагностики сбоев в Kaspersky Security Center
Работа с расписанием задач
Настройка расписания запуска задач
Включение и выключение запуска задач по расписанию
Отчеты в Kaspersky Security Center
Диагностическое окно
О диагностическом окне
Просмотр состояния Kaspersky Embedded Systems Security с помощью диагностического окна
Просмотр статистики событий безопасности
Просмотр текущей активности программы
Настройка записи файлов дампов и файлов трассировки
Обновление баз и модулей Kaspersky Embedded Systems Security
О задачах обновления
Об обновлении модулей программы
Об обновлении баз программы
Схемы обновления баз и модулей антивирусных программ в организации
Настройка задач обновления
Настройка параметров работы с источниками обновлений Kaspersky Embedded Systems Security
Оптимизация дисковой подсистемы при выполнении задачи Обновление баз программы
Настройка параметров задачи Копирование обновлений
Настройка параметров задачи Обновление модулей программы
Откат обновления баз Kaspersky Embedded Systems Security
Откат обновления программных модулей
Статистика задач обновления
Изолирование и резервное копирование объектов
Изолирование возможно зараженных объектов. Карантин
Об изолировании возможно зараженных объектов
Просмотр объектов на карантине
Сортировка объектов на карантине
Фильтрация объектов на карантине
Проверка объектов на карантине
Восстановление содержимого карантина
Помещение объектов на карантин
Удаление объектов с карантина
Отправка возможно зараженных объектов на исследование в "Лабораторию Касперского"
Настройка параметров карантина
Статистика карантина
Резервное копирование объектов. Резервное хранилище
О резервном копировании объектов перед лечением или удалением
Просмотр объектов в резервном хранилище
Сортировка файлов в резервном хранилище
Фильтрация файлов в резервном хранилище

Восстановление файлов из резервного хранилища
Удаление файлов из резервного хранилища
Настройка параметров резервного хранилища
Статистика резервного хранилища
Блокировка доступа к сетевым ресурсам. Заблокированные узлы
О хранилище заблокированных узлов
Управление заблокированными узлами с помощью Плагина управления
Включение блокировки недоверенных узлов
Настройка параметров хранилища заблокированных узлов
Управление заблокированными узлами с помощью Консоли программы
Включение блокировки недоверенных узлов
Настройка параметров хранилища заблокированных узлов
Управление заблокированными узлами с помощью Веб-плагина
Включение блокировки узлов
Настройка параметров хранилища заблокированных узлов
Запись событий. Журналы Kaspersky Embedded Systems Security
Способы записи событий Kaspersky Embedded Systems Security
Журнал системного аудита
Сортировка событий в журнале системного аудита
Фильтрация событий в журнале системного аудита
Удаление событий из журнала системного аудита
Журналы выполнения задач
О журналах выполнения задач
Просмотр списка событий в журналах выполнения задач
Сортировка журналов выполнения задач
Фильтрация журналов выполнения задач
Просмотр статистики и информации о задачах Kaspersky Embedded Systems Security в журналах выполнения задач
Экспорт информации из журнала выполнения задачи
Удаление журналов выполнения задач
Журнал безопасности
Просмотр журнала событий Kaspersky Embedded Systems Security в оснастке Просмотр событий
Настройка параметров журналов с помощью Плагина управления
Об интеграции с SIEM
Настройка параметров интеграции с SIEM
Настройка журналов и уведомлений
Настройка параметров журналов
Журнал безопасности
Настройка параметров интеграции с SIEM
Настройка параметров уведомлений
Настройка обмена информацией с Сервером администрирования
Настройка уведомлений
Способы уведомления администратора и пользователей
Настройка уведомлений администратора и пользователей
Запуск и остановка Kaspersky Embedded Systems Security
Запуск Плагина управления Kaspersky Embedded Systems Security
Запуск Консоли Kaspersky Embedded Systems Security из меню Пуск
Запуск и остановка службы Kaspersky Security
Запуск компонентов Kaspersky Embedded Systems Security при безопасном режиме загрузки операционной системы

- О работе Kaspersky Embedded Systems Security при безопасном режиме загрузки операционной системы
- Запуск Kaspersky Embedded Systems Security в безопасном режиме

Механизмы самозащиты Kaspersky Embedded Systems Security

- О механизмах самозащиты Kaspersky Embedded Systems Security
- Защита от изменений папок с установленными компонентами Kaspersky Embedded Systems Security
- Защита от изменений ключей реестра Kaspersky Embedded Systems Security
- Регистрация службы Kaspersky Security как защищенной службы
- Управление правами доступа к функциям Kaspersky Embedded Systems Security
  - О правах на управление Kaspersky Embedded Systems Security
  - О правах на управление регистрируемыми службами
  - О правах доступа к службе Kaspersky Security Management
  - О правах на управление службой Kaspersky Security
  - Управление правами доступа с помощью Плагина управления
    - Настройка прав доступа к Kaspersky Embedded Systems Security и службе Kaspersky Security
    - Защита доступа к функциям Kaspersky Embedded Systems Security с помощью пароля
  - Управление правами доступа с помощью Консоли программы
    - Настройка прав доступа на управление Kaspersky Embedded Systems Security и службой Kaspersky Security
    - Защита доступа к функциям Kaspersky Embedded Systems Security с помощью пароля
  - Управление правами доступа с помощью Веб-плагина
    - Настройка прав доступа к Kaspersky Embedded Systems Security и службе Kaspersky Security
    - Защита доступа к функциям Kaspersky Embedded Systems Security с помощью пароля

Постоянная защита файлов

- О задаче Постоянная защита файлов
- Об области защиты и параметрах безопасности задачи
- О виртуальной области защиты
- Стандартные области защиты
- Стандартные уровни безопасности
- Расширения файлов, проверяемые по умолчанию в задаче Постоянная защита файлов
- Параметры задачи Постоянная защита файлов по умолчанию
- Управление задачей Постоянная защита файлов с помощью Плагина управления
  - Навигация
    - Переход к параметрам политики для задачи Постоянная защита файлов
    - Переход к параметрам задачи Постоянная защита файлов
  - Настройка задачи Постоянная защита файлов
    - Выбор режима защиты
    - Настройка эвристического анализатора и интеграции с другими компонентами программы
    - Настройка расписания запуска задач
  - Создание и настройка области защиты задачи
  - Выбор стандартных уровней безопасности в задачах проверки по требованию
  - Настройка параметров безопасности вручную
    - Настройка общих параметров задачи
    - Настройка действий
    - Настройка производительности
- Управление задачей Постоянная защита файлов с помощью Консоли программы
  - Навигация
    - Переход к параметрам задачи Постоянная защита файлов
    - Переход к параметрам области действия задачи Постоянная защита файлов
  - Настройка задачи Постоянная защита файлов

Выбор режима защиты объектов
Настройка эвристического анализатора и интеграции с другими компонентами программы
Настройка расписания запуска задач
Формирование области защиты
Настройка отображения сетевых файловых ресурсов
Формирование области защиты
Включение сетевых объектов в область защиты
Формирование виртуальной области защиты
Настройка параметров безопасности вручную
Выбор стандартных уровней безопасности в задаче Постоянная защита файлов
Настройка общих параметров задачи
Настройка действий
Настройка производительности
Статистика задачи Постоянная защита файлов
Управление задачей Постоянная защита файлов с помощью Веб-плагина
Использование KSN
О задаче Использование KSN
Параметры по умолчанию для задачи Использование KSN
Управление использованием KSN с помощью Плагина управления
Настройка параметров задачи Использование KSN
Настройка обработки данных
Управление использованием KSN с помощью Консоли программы
Настройка параметров задачи Использование KSN
Настройка обработки данных
Управление использованием KSN с помощью Веб-плагина
Настройка передачи дополнительных данных
Статистика задачи Использование KSN
Защита от сетевых угроз
О задаче Защита от сетевых угроз
Параметры по умолчанию для задачи Защита от сетевых угроз
Настройка задачи Защита от сетевых угроз с помощью Консоли программы
Общие параметры задачи
Добавление исключений
Настройка задачи Защита от сетевых угроз с помощью Плагина управления
Общие параметры задачи
Добавление исключений
Настройка задачи Защита от сетевых угроз с помощью Веб-плагина
Общие параметры задачи
Добавление исключений
Контроль запуска программ
О задаче Контроль запуска программ
О правилах контроля запуска программ
О Контроле пакетов установки
Об использовании KSN в задаче Контроль запуска программ
О формировании правил контроля запуска программ
Параметры по умолчанию для задачи Контроль запуска программ
Управление контролем запуска программ с помощью Плагина управления
Навигация

Переход к параметрам политики для задачи Контроль запуска программ
Переход к списку правил контроля запуска программ
Переход к мастеру создания задачи Формирование правил контроля запуска программ и ее свойствам
Настройка параметров задачи Контроль запуска программ
Настройка Контроля пакетов установки
Настройка задачи Формирование правил контроля запуска программ
Настройка правил контроля запуска программ в Kaspersky Security Center
Добавление правила контроля запуска программ
Включение режима разрешения по умолчанию
Создание разрешающих правил на основе событий Kaspersky Security Center
Импорт правил из отчета Kaspersky Security Center о заблокированных программах
Импорт правил контроля запуска программ из XML-файла
Проверка запуска программ
Создание задачи Формирование правил контроля запуска программ
Ограничение области действия задачи
Действия при автоматическом формировании правил
Действия по завершении автоматического формирования правил
Управление контролем запуска программ с помощью Консоли программы
Навигация
Переход к параметрам задачи Контроль запуска программ
Переход к окну с правилами контроля запуска программ
Переход к параметрам задачи Формирование правил контроля запуска программ
Настройка параметров задачи Контроль запуска программ
Выбор режима работы задачи Контроль запуска программ
Настройка области действия задачи Контроль запуска программ
Настройка использования KSN
Контроль пакетов установки
Настройка правил контроля запуска программ
Добавление правила контроля запуска программ
Включение режима разрешения по умолчанию
Формирование разрешающих правил по событиям задачи Контроль запуска программ
Экспорт правил контроля запуска программ
Импорт правил контроля запуска программ из XML-файла
Удаление правил контроля запуска программ
Настройка задачи Формирование правил контроля запуска программ
Ограничение области действия задачи
Действия при автоматическом формировании правил
Действия по завершении автоматического формирования правил
Управление контролем запуска программ с помощью веб-плагина
Контроль устройств
О задаче Контроль устройств
О правилах контроля устройств
О формировании правил контроля устройств
О задаче Формирование правил контроля устройств
Параметры по умолчанию для задачи Контроль устройств
Управление контролем устройств с помощью Плагина управления
Навигация
Переход к параметрам политики для задачи Контроль устройств

Переход к списку правил контроля устройств
Переход к мастеру создания задачи Формирование правил контроля устройств и ее свойствам
Настройка задачи Контроль устройств
Настройка задачи Формирование правил контроля устройств
Настройка правил контроля устройств в Kaspersky Security Center
Формирование разрешающих правил на основе данных системы в политике Kaspersky Security Center
Формирование правил для подключенных устройств
Импорт правил из отчета Kaspersky Security Center о заблокированных устройствах
Создание правил с помощью задачи Формирование правил контроля устройств
Добавление сформированных правил в список правил контроля устройств
Управление Контролем устройств с помощью Консоли программы
Навигация
Переход к параметрам задачи Контроль устройств
Переход к окну с правилами контроля устройств
Переход к параметрам задачи Формирование правил контроля устройств
Настройка параметров задачи Контроль устройств
Настройка правил контроля устройств
Импорт правил контроля устройств из файла формата XML
Формирование списка правил по событиям задачи Контроль устройств
Добавление разрешающего правила для одного или нескольких внешних устройств
Удаление правил контроля устройств
Экспорт правил контроля устройств
Активация и выключение правила контроля устройств
Расширение области применения правил контроля устройств
Настройка задачи Формирование правил контроля устройств
Управление Контролем устройств с помощью Веб-плагина Консоли программы-
Управление сетевым экраном
О задаче Управление сетевым экраном
О правилах сетевого экрана
Параметры по умолчанию для задачи Управление сетевым экраном
Управление правилами сетевого экрана с помощью Плагина управления
Включение и выключение правил сетевого экрана
Добавление правил сетевого экрана вручную
Удаление правил сетевого экрана
Управление правилами сетевого экрана с помощью Консоли программы
Включение и выключение правил сетевого экрана
Добавление правил сетевого экрана вручную
Удаление правил сетевого экрана
Управление правилами сетевого экрана с помощью Веб-плагина
Включение и выключение правил сетевого экрана
Добавление правил сетевого экрана вручную
Удаление правил сетевого экрана
Мониторинг файловых операций
О задаче Мониторинг файловых операций
О правилах мониторинга файловых операций
Параметры по умолчанию для задачи Мониторинг файловых операций
Управление мониторингом файловых операций с помощью Плагина управления
Настройка задачи Мониторинг файловых операций

- Настройка правил мониторинга
- Управление мониторингом файловых операций с помощью Консоли программы
  - Настройка параметров задачи Мониторинг файловых операций
  - Настройка правил мониторинга
- Управление мониторингом файловых операций с помощью Веб-плагина
  - Настройка задачи Мониторинг файловых операций
  - Настройка правил мониторинга

Анализ журналов

- О задаче Анализ журналов
- Параметры по умолчанию для задачи Анализ журналов
- Управление правилами анализа журналов с помощью Плагина управления
  - Настройка параметров предзаданных правил задачи
  - Добавление правил анализа журналов с помощью Плагина управления
- Управление правилами анализа журналов с помощью Консоли программы
  - Настройка параметров предзаданных правил задачи
  - Добавление правил анализа журналов с помощью Консоли программы
- Управление правилами анализа журналов с помощью Веб-плагина

Проверка по требованию

- О задачах проверки по требованию
- Об области проверки и параметрах безопасности задачи
- Стандартные области проверки
- Проверка файлов в интернет-хранилище
- Стандартные уровни безопасности
- Проверка съемных дисков
- О задаче Мониторинг целостности файлов на основе эталона
- Включение запуска задачи проверки по требованию из контекстного меню
- Заданные по умолчанию параметры задач проверки по требованию
- Управление задачами проверки по требованию с помощью Плагина управления
  - Навигация
    - Переход к мастеру создания задачи проверки по требованию
    - Переход к свойствам задачи проверки по требованию
  - Создание задачи проверки по требованию
    - Присвоение задаче проверки по требованию статуса Проверка важных областей
    - Выполнение задач проверки по требованию в фоновом режиме
    - Регистрация выполнения задачи Проверка важных областей
  - Настройка области проверки для задачи
  - Выбор стандартных уровней безопасности в задачах проверки по требованию
  - Настройка параметров безопасности вручную
    - Настройка общих параметров задачи
    - Настройка действий
    - Настройка производительности
  - Настройка проверки съемных дисков
  - Настройка задачи Мониторинг целостности файлов на основе эталона
- Управление задачами проверки по требованию с помощью Консоли программы
  - Навигация
    - Переход к параметрам задачи проверки по требованию
    - Переход к параметрам области действия задачи проверки по требованию
  - Создание и настройка задачи проверки по требованию

Область проверки в задачах проверки по требованию
Настройка отображения сетевых файловых ресурсов
Формирование области проверки
Включение в область проверки сетевых объектов
Создание виртуальной области проверки
Настройка параметров безопасности
Выбор стандартных уровней безопасности в задачах проверки по требованию
Настройка общих параметров задачи
Настройка действий
Настройка производительности
Настройка иерархического хранилища
Проверка съемных дисков
Статистика задач проверки по требованию
Создание и настройка задачи Мониторинг целостности файлов на основе эталона
Управление задачами проверки по требованию с помощью Веб-плагина
Переход к мастеру создания задачи проверки по требованию
Переход к свойствам задачи проверки по требованию
Доверенная зона
О доверенной зоне
Управление доверенной зоной с помощью Плагина управления
Навигация
Переход к параметрам политики для доверенной зоны
Переход к окну параметров доверенной зоны
Настройка параметров доверенной зоны с помощью Плагина управления
Добавление исключений
Добавление доверенных процессов
Использование маски not-a-virus
Управление доверенной зоной с помощью Консоли программы
Использование доверенной зоны для задач в Консоли программы
Настройка параметров доверенной зоны в Консоли программы
Добавление исключений в доверенную зону
Добавление доверенных процессов
Использование маски not-a-virus
Управление доверенной зоной с помощью Веб-плагина
Защита от эксплойтов
О защите от эксплойтов
Управление защитой от эксплойтов с помощью Плагина управления
Навигация
Переход к параметрам политики для защиты от эксплойтов
Переход к окну параметров защиты от эксплойтов
Настройка защиты памяти процессов
Добавление процесса в область защиты
Управление защитой от эксплойтов с помощью Консоли программы
Навигация
Переход к основным параметрам защиты от эксплойтов
Переход к параметрам защиты процессов при защите от эксплойтов
Настройка защиты памяти процессов
Добавление процесса в область защиты

Управление защитой от эксплойтов с помощью Веб-плагина
Настройка защиты памяти процессов
Добавление процесса в область защиты
Техники защиты от эксплойтов
Интеграция со сторонними системами
Счетчики производительности для программы Системный монитор
О счетчиках производительности Kaspersky Embedded Systems Security
Общее количество отвергнутых запросов
Общее количество пропущенных запросов
Количество запросов, не обработанных из-за нехватки системных ресурсов
Количество запросов, отправленных на обработку
Среднее количество потоков диспетчера файловых перехватов
Максимальное количество потоков диспетчера файловых перехватов
Количество элементов в очереди зараженных объектов
Количество объектов, обрабатываемых за секунду
Счетчики и ловушки SNMP Kaspersky Embedded Systems Security
О счетчиках и ловушках SNMP Kaspersky Embedded Systems Security
SNMP-счетчики Kaspersky Embedded Systems Security
Счетчики производительности
Счетчики карантина
Счетчик резервного хранилища
Общие счетчики
Счетчик обновлений
Счетчики постоянной защиты файлов
SNMP-ловушки Kaspersky Embedded Systems Security и их параметры
Описания и возможные значения параметров SNMP-ловушек Kaspersky Embedded Systems Security
Интеграция с WMI
Работа с Kaspersky Embedded Systems Security из командной строки
Команды
Вызов справки о командах Kaspersky Embedded Systems Security: KAVSHELL HELP
Запуск и остановка службы Kaspersky Security. KAVSHELL START, KAVSHELL STOP
Проверка выбранной области. KAVSHELL SCAN
Запуск задачи Проверка важных областей. KAVSHELL SCANCRITICAL
Управление задачей в асинхронном режиме. KAVSHELL TASK
Удаление атрибута защищенного процесса (PPL): KAVSHELL CONFIG
Запуск и остановка задач постоянной защиты компьютера. KAVSHELL RTP
Управление задачей Контроль запуска программ. KAVSHELL APPCONTROL /CONFIG
Формирование правил контроля запуска программ. KAVSHELL APPCONTROL /GENERATE
Наполнение списка правил контроля запуска программ. KAVSHELL APPCONTROL
Наполнение списка правил контроля устройств. KAVSHELL DEVCONTROL
Запуск задачи Обновление баз программы. KAVSHELL UPDATE
Откат обновления баз Kaspersky Embedded Systems Security. KAVSHELL ROLLBACK
Управление анализом журналов. KAVSHELL TASK LOG-INSPECTOR
Включение, настройка и выключение журналов трассировки. KAVSHELL TRACE
Дефрагментация файлов журналов Kaspersky Embedded Systems Security: KAVSHELL VACUUM
Очищение базы iSwift. KAVSHELL FBRESET
Включение и выключение создания файла дампа. KAVSHELL DUMP
Импорт параметров. KAVSHELL IMPORT

Экспорт параметров. KAVSHELL EXPORT
Интеграция с Microsoft Operations Management Suite. KAVSHELL OMSINFO
Управление задачей Мониторинг целостности файлов на основе эталона: KAVSHELL FIM /BASELINE
Коды возврата команд
Коды возврата команд KAVSHELL START и KAVSHELL STOP
Коды возврата команд KAVSHELL SCAN и KAVSHELL SCANCRITICAL
Коды возврата команды KAVSHELL TASK LOG-INSPECTOR
Коды возврата команды KAVSHELL TASK
Коды возврата команды KAVSHELL RTP
Коды возврата команды KAVSHELL UPDATE
Коды возврата команды KAVSHELL ROLLBACK
Коды возврата команды KAVSHELL LICENSE
Коды возврата команды KAVSHELL TRACE
Коды возврата команды KAVSHELL FBRESET
Коды возврата команды KAVSHELL DUMP
Коды возврата команды KAVSHELL IMPORT
Коды возврата команды KAVSHELL EXPORT
Коды возврата команды KAVSHELL FIM /BASELINE
Обращение в Службу технической поддержки
Способы получения технической поддержки
Получение технической поддержки по телефону
Техническая поддержка через Kaspersky CompanyAccount
Использование файла трассировки и скрипта AVZ
Глоссарий
Kaspersky Security Network (KSN)
OLE-объект
SIEM
Активный ключ
Антивирусные базы
Архив
Задача
Зараженный объект
Карантин
Лечение объектов
Ложное срабатывание
Локальная задача
Маска файла
Обновление
Объекты автозапуска
Параметры задачи
Политика
Потенциально заражаемый файл
Резервное хранилище
Сервер администрирования
Срок действия лицензии
Статус защиты
Уровень безопасности
Уровень важности события

Уязвимость
Эвристический анализатор
Информация о стороннем коде
Уведомления о товарных знаках

О Kaspersky Embedded Systems Security

Kaspersky Embedded Systems Security защищает компьютеры и другие встроенные системы под управлением операционной системы Microsoft® Windows® (защищаемые устройства) от вирусов и прочих угроз компьютерной безопасности. Пользователями Kaspersky Embedded Systems Security являются администраторы сети организации и сотрудники, отвечающие за антивирусную защиту сети организации.

Kaspersky Embedded Systems Security можно установить на различные встроенные системы под управлением Windows, включая устройства следующих типов:

- банковские автоматы;
- POS-терминалы.

Вы можете управлять Kaspersky Embedded Systems Security следующими способами:

- с помощью Консоли программы, установленной на одном защищаемом устройстве с Kaspersky Embedded Systems Security или на другом устройстве;
- с помощью команд командной строки;
- с помощью Консоли администрирования Kaspersky Security Center.

Вы можете использовать программу Kaspersky Security Center для централизованного управления защищаемыми устройствами с установленной программой Kaspersky Embedded Systems Security.

Вы можете просматривать счетчики производительности Kaspersky Embedded Systems Security для программы Системный монитор, а также счетчики и ловушки SNMP.

Компоненты и функции Kaspersky Embedded Systems Security

В состав программы входят следующие компоненты:

- **Постоянная защита файлов**. Kaspersky Embedded Systems Security проверяет объекты при обращении к ним. Kaspersky Embedded Systems Security проверяет следующие объекты:
  - файлы;
  - альтернативные потоки файловых систем (NTFS-streams);
  - Основные загрузочные записи и загрузочные секторы локальных жестких и съемных дисков.
- **Проверка по требованию**. Kaspersky Embedded Systems Security однократно проверяет указанную область на наличие вирусов и других угроз компьютерной безопасности. Программа проверяет файлы, оперативную память и объекты автозапуска на защищаемом устройстве.
- **Контроль запуска программ**. Компонент отслеживает попытки запуска программ пользователями и регулирует запуск программ на защищаемом устройстве.
- **Контроль устройств**. Компонент позволяет контролировать регистрацию и использование внешних устройств с целью защиты устройства от угроз компьютерной безопасности, которые могут возникнуть во время файлового обмена с USB-подключаемым флеш-накопителем или внешними устройствами других типов.

- **Управление сетевым экраном**. Этот компонент обеспечивает возможность управления брандмауэром Windows: позволяет настраивать параметры и правила сетевого экрана операционной системы и блокирует любую возможность настройки параметров сетевого экрана извне.

- **Мониторинг файловых операций**. Kaspersky Embedded Systems Security обнаруживает изменения в файлах из области мониторинга, указанной в параметрах задачи. Эти изменения указывают на нарушение безопасности на защищаемом устройстве.

- **Анализ журналов**. Компонент выполняет контроль целостности защищаемой среды на основе результатов анализа журналов событий Windows.

В программе реализованы следующие функции:

- **Обновление баз программы** и **Обновление модулей программы**. Kaspersky Embedded Systems Security загружает обновления баз и модулей программы с FTP- или HTTP-серверов обновлений "Лаборатории Касперского", Сервера администрирования Kaspersky Security Center или из других источников обновлений.

- **Карантин** Kaspersky Embedded Systems Security перемещает объекты, которые признает возможно зараженными, из исходного местоположения в папку *Карантин*. В целях безопасности объекты, помещенные на карантин, хранятся в зашифрованном виде.

- **Резервное хранилище**. Kaspersky Embedded Systems Security сохраняет зашифрованные копии объектов со статусом *зараженный* в папке *Резервное хранилище* перед тем, как выполнить лечение или удаление этих объектов.

- **Уведомления администратора и пользователей**. Вы можете настроить уведомление администратора и пользователей, которые обращаются к защищаемому устройству, о событиях, связанных с работой Kaspersky Embedded Systems Security и состоянии антивирусной защиты устройства.

- **Импорт и экспорт параметров**. Вы можете экспортировать параметры Kaspersky Embedded Systems Security в конфигурационный файл в формате XML и импортировать параметры в Kaspersky Embedded Systems Security из конфигурационного файла. Вы можете сохранить в конфигурационный файл как все параметры программы, так и параметры ее отдельных компонентов.

- **Применение шаблонов**. Вы можете вручную настроить параметры безопасности узла в дереве или списке файловых ресурсов защищаемого устройства и сохранить значения настроенных параметров в шаблон. Затем вы можете применить этот шаблон при настройке параметров безопасности других узлов в задачах защиты и проверки Kaspersky Embedded Systems Security.

- **Управление правами доступа к функциям Kaspersky Embedded Systems Security.** Вы можете настраивать права на управление Kaspersky Embedded Systems Security и службами Windows, которые регистрирует программа, для пользователей и групп пользователей.

- **Запись событий в журнал событий Windows**. Kaspersky Embedded Systems Security записывает в журнал событий информацию о параметрах функциональных компонентов программы, текущем состоянии задач, событиях, возникших за время их выполнения, а также о событиях, связанных с управлением Kaspersky Embedded Systems Security, и информацию, необходимую для диагностики сбоев в работе программы.

- **Доверенная зона**. Вы можете сформировать список исключений из области защиты или проверки, который Kaspersky Embedded Systems Security будет применять в задачах проверки по требованию и постоянной защиты компьютера.

- **Защита от эксплойтов**. Вы можете защищать память процессов от эксплуатации уязвимостей с помощью внедряемого в процессы Агента защиты.

Что нового

В новой версии Kaspersky Embedded Systems Security появились следующие возможности:

- Защита от сетевых угроз: реализован компонент, обеспечивающий анализ входящего трафика на наличие признаков сетевых атак. В случае обнаружения угрозы, компонент Защита от сетевых угроз блокирует скомпрометированный IP-адрес.

- Добавлена возможность использования программы в режиме Long Term. Теперь можно активировать программу на длительный срок, в течение которого программа будет контролировать запуски запрещенных программ.

- Профили политики Kaspersky Security Center для списков Доверенной зоны: теперь вы можете сформировать профили политики для списков доверенных процессов и списков исключений Доверенной зоны с помощью Плагина управления версии 3.0.

- Мониторинг изменения файлов по требованию на основе криптографии: программа позволяет сформировать эталонные списки файлов и запускать проверки соответствия файлов на диске параметрам, зафиксированным в эталоне. Программа обнаруживает следующие несовпадения с эталоном: создание новых файлов в контролируемых областях, удаление файлов в контролируемых областях, изменение контрольной суммы контролируемого файла.

- Контроль подключения сетевых карт и модемов: задачи Контроль устройств и Автоматическое формирование правил контроля устройств поддерживают создание и применение правил, запрещающих подключение недоверенных сетевых карт и модемов по USB.

- В событиях обнаружения, которые публикуются в отчетах Kaspersky Security Center, добавлена информация о контрольной сумме обрабатываемого объекта.

- Реализован Веб-плагин управления: теперь вы можете управлять программой с помощью Веб-консоли Kaspersky Security Center.

- Формирование инцидентов Kaspersky Security Center по событиям блокировки запуска программ и подключения устройств в режиме аудита.

- Блокировка изменений важных параметров журнала USN (Update Sequence Number): программа использует записи журнала USN для мониторинга файловых операций. Вы можете запретить удаление записей из журнала USN и изменять пороговое значение максимального размера журнала USN.

- Уведомление об изменениях важных параметров журнала USN (Update Sequence Number): если вы не включили запрет на изменение важных параметров журнала USN, программа будет сообщать о попытках удаления записей из журнала USN посредством публикации событий в отчеты программы.

- Оптимизированы способы защиты от активных угроз: теперь программа уведомит вас, если в ходе выполнения задач постоянной защиты были обнаружены признаки активного заражения. Программа отметит обнаруженные объекты для удаления и удалит их с компьютера после перезагрузки.

- Добавлена возможность в параметрах задачи постоянной защиты включить запуск задачи Проверка важных областей при обнаружении признаков активного заражения. Если этот параметр включен, программа будет автоматически создавать и запускать временную задачу Проверка важных областей на компьютере, где было обнаружено активное заражение.

- Реализована антивирусная проверка задач, созданных в системном Планировщике. Проверка задач, созданных в системном Планировщике, выполняется в рамках задач проверки по требованию с включенной областью проверки "Объекты автозапуска".

- Реализована обработка постоянных подписок WMI: теперь программа обнаруживает подозрительные подписки WMI в пространстве имен WMI на компьютере с установленной программой Kaspersky Embedded Systems Security и удаляет их. Проверка постоянных подписок WMI выполняется в рамках задач проверки по требованию с включенной областью проверки "Объекты автозапуска".

- Расширены критерии срабатывания пользовательских правил для компонента Анализ журналов: теперь вы можете задавать правила по значению параметра "Источник" в журнале событий Windows.

- Добавлена возможность настраивать критерии срабатывания правила контроля запуска программ при создании правил на основе событий блокировки запуска программ в консоли Kaspersky Security Center.

- Расширены опции ротации файлов журналов трассировки.

- Расширен список поддерживаемых операционных систем.

- Интерфейс программы приведен в соответствие новой бренд-политике компании.

- Исправлены ошибки предыдущих версий: в программу вошли исправления, выпущенные для предыдущих версий программы.

Источники информации о Kaspersky Embedded Systems Security

Этот раздел содержит описание источников информации о программе.

Вы можете выбрать наиболее удобный источник информации в зависимости от важности и срочности вопроса.

Источники для самостоятельного поиска информации

Вы можете использовать следующие источники для самостоятельного поиска информации о Kaspersky Embedded Systems Security:

- страница Kaspersky Embedded Systems Security на веб-сайте "Лаборатории Касперского";
- страница программы на веб-сайте Службы технической поддержки (База знаний);
- документация.

Если вы не нашли решения своей проблемы, обратитесь в Службу технической поддержки "Лаборатории Касперского".

Для использования источников информации на веб-сайтах требуется подключение к интернету.

Страница Kaspersky Embedded Systems Security на веб-сайте "Лаборатории Касперского"

На странице Kaspersky Embedded Systems Security можно ознакомиться с общей информацией о программе, ее возможностях и особенностях работы.

Страница Kaspersky Embedded Systems Security содержит ссылку на интернет-магазин. В нем вы можете приобрести программу или продлить право пользования программой.

Страница Kaspersky Embedded Systems Security в Базе знаний

База знаний – это раздел веб-сайта Службы технической поддержки.

На странице Kaspersky Embedded Systems Security в Базе знаний приведены статьи, которые содержат полезную информацию, рекомендации и ответы на часто задаваемые вопросы о приобретении, установке и использовании программы.

Статьи Базы знаний могут отвечать на вопросы, относящиеся не только к Kaspersky Embedded Systems Security, но и к другим программам "Лаборатории Касперского". Статьи Базы знаний также могут содержать новости Службы технической поддержки.

Документация Kaspersky Embedded Systems Security

В Руководстве администратора Kaspersky Embedded Systems Security вы можете найти информацию об установке, удалении, настройке и использовании программы.

Обсуждение программ "Лаборатории Касперского" в сообществе пользователей

Если ваш вопрос не требует срочного ответа, вы можете обсудить его со специалистами "Лаборатории Касперского" и другими пользователями в нашем сообществе.

В сообществе вы можете просматривать опубликованные темы, добавлять свои комментарии, создавать новые темы для обсуждения.

Kaspersky Embedded Systems Security

Этот раздел содержит описание функций, компонентов и комплекта поставки Kaspersky Embedded Systems Security, перечень аппаратных и программных требований Kaspersky Embedded Systems Security.

Комплект поставки

В комплект поставки входит программа-приветствие, из которой вы можете выполнить следующие действия:

- запустить мастер установки Kaspersky Embedded Systems Security;
- запустить мастер установки Консоли Kaspersky Embedded Systems Security;
- запустить мастер установки Плагина управления Kaspersky Embedded Systems Security, который позволяет управлять программой через Kaspersky Security Center;
- прочитать Руководство администратора;
- перейти на страницу Kaspersky Embedded Systems Security на веб-сайте "Лаборатории Касперского";
- перейти на веб-сайт Службы технической поддержки;
- прочитать информацию о текущем выпуске Kaspersky Embedded Systems Security.

Папка \console содержит файлы для установки Консоли программы (набор компонентов Средства Администрирования Kaspersky Embedded Systems Security).

Папка \product содержит следующие файлы:

- файлы для установки компонентов Kaspersky Embedded Systems Security на защищаемое устройстве под управлением 32-разрядной или 64-разрядной операционной системы Microsoft Windows;
- файл для установки Плагина управления Kaspersky Embedded Systems Security через Kaspersky Security Center;
- архив антивирусных баз, актуальных на момент выпуска программы;
- файл с текстом Лицензионного соглашения и Политики конфиденциальности.

Папка \product_long_term содержит файлы установки компонентов Kaspersky Embedded Systems Security и Плагина управления без антивирусных баз.

Папка \setup содержит файлы, необходимые для запуска программы-приветствия.

Файлы комплекта поставки располагаются в разных папках в зависимости от их предназначения (см. таблицу ниже).

Файлы комплекта поставки Kaspersky Embedded Systems Security

Файл	Назначение
autorun.inf	Файл автозапуска мастера установки Kaspersky Embedded Systems Security при установке программы со съемных дисков.
release_notes.txt	Файл содержит информацию о версии.

migration.txt	Файл с описанием перехода с предыдущих версий программы.
setup.exe	Файл запуска программы приветствия (запускает setup.hta).
\console\esstools_x86.msi	Пакет установщика Windows. Устанавливает Консоль программы на управляемое устройство с 32-разрядной операционной системой Microsoft Windows.
\console\esstools_x64.msi	Пакет установщика Windows. Устанавливает Консоль программы на управляемое устройство с 64-разрядной операционной системой Microsoft Windows.
\console\setup.exe	Файл запуска мастера установки для набора компонентов Средства администрирования (включающего в себя Консоль программы); запускает файл пакета установки esstools.msi с указанными в мастере параметрами установки.
\product\bases.cab	Архив антивирусных баз, актуальных на момент выпуска программы.
\product\setup.exe	Файл для установки Kaspersky Embedded Systems Security на защищаемом устройстве с помощью мастера установки; запускает файл пакета установки ess.msi с указанными в мастере параметрами.
\product\ess_x86.msi	Пакет установщика Windows. Устанавливает Kaspersky Embedded Systems Security в конфигурации **Защита компьютера с помощью антивирусных баз** на защищаемое устройство с 32-разрядной операционной системой Microsoft Windows. Если выбрана конфигурация "Защита компьютера с помощью антивирусных баз", все компоненты Kaspersky Embedded Systems Security, кроме компонентов Управление сетевым экраном и Счетчики производительности, включены по умолчанию. При установке Kaspersky Embedded Systems Security в конфигурации "Защита компьютера с помощью антивирусных баз" поверх версии программы, в которой не используется сигнатурный анализ и антивирусные базы для защиты компьютера, набор компонентов программы будет автоматически расширен за счет добавления следующих компонентов: • Постоянная защита файлов • Проверка по требованию • Защита от сетевых угроз
\product\ess_x64.msi	Пакет установщика Windows. Устанавливает Kaspersky Embedded Systems Security в конфигурации **Защита компьютера с помощью антивирусных баз** на защищаемое устройство с 64-разрядной операционной системой Microsoft Windows.

	Если выбрана конфигурация "Защита компьютера с помощью антивирусных баз", все компоненты Kaspersky Embedded Systems Security, кроме компонентов Управление сетевым экраном и Счетчики производительности, включены по умолчанию. При установке Kaspersky Embedded Systems Security в конфигурации "Защита компьютера с помощью антивирусных баз" поверх версии программы, в которой не используется сигнатурный анализ и антивирусные базы для защиты компьютера, набор компонентов программы будет автоматически расширен за счет добавления следующих компонентов: • Постоянная защита файлов • Проверка по требованию • Защита от сетевых угроз
\product\ess.kud	Файл в формате Kaspersky Unicode Definition с описанием пакета установки для удаленной установки Kaspersky Embedded Systems Security через Kaspersky Security Center.
\product\klcfginst.exe	Программа установки Плагина управления Kaspersky Embedded Systems Security через Kaspersky Security Center. Установите Плагин управления на каждом защищаемом устройстве, на котором установлена Консоль администрирования Kaspersky Security Center, если вы планируете управлять Kaspersky Embedded Systems Security через нее.
\product\license.txt	Файл с текстом Лицензионного соглашения и Политики конфиденциальности.
\product_long_term\setup.exe	Файл для установки Kaspersky Embedded Systems Security на защищаемом устройстве с помощью мастера установки; запускает файл пакета установки ess.msi с указанными в мастере параметрами.
\product_long_term\ess_x86.msi	Пакет установщика Windows. Устанавливает Kaspersky Embedded Systems Security в конфигурации **Защита компьютера с помощью технологии "запрет по умолчанию"** на защищаемое устройство с 32-разрядной операционной системой Microsoft Windows.

	Компоненты, отвечающие за обновления, не входят в конфигурацию "Защита компьютера с помощью технологии "запрет по умолчанию". Если выбрана конфигурация "Защита компьютера с помощью технологии "запрет по умолчанию", то по умолчанию включены следующие компоненты: • Core • Защита от эксплойтов • Контроль запуска программ • Значок области уведомлений При установке Kaspersky Embedded Systems Security в конфигурации "Защита компьютера с помощью технологии "запрет по умолчанию" поверх версии программы, в которой используются сигнатурный анализ и антивирусные базы для защиты компьютера, набор компонентов программы будет автоматически сокращен за счет удаления следующих компонентов: • Постоянная защита файлов • Проверка по требованию • Компоненты, отвечающие за обновления Рекомендуется использовать эту конфигурацию для защиты систем с ограниченными ресурсами. В этом случае вы сможете активировать программу на длительный срок, а компонент Контроль запуска программ обеспечит защиту компьютера.
\product_long_term\ess_x64.msi	Пакет установщика Windows. Устанавливает Kaspersky Embedded Systems Security в конфигурации **Защита компьютера с помощью технологии "запрет по умолчанию"** на защищаемое устройство с 64-разрядной операционной системой Microsoft Windows.

	Компоненты, отвечающие за обновления, не входят в конфигурацию "Защита компьютера с помощью технологии "запрет по умолчанию". Если выбрана конфигурация "Защита компьютера с помощью технологии "запрет по умолчанию", то по умолчанию включены следующие компоненты: • Core • Защита от эксплойтов • Контроль запуска программ • Значок области уведомлений При установке Kaspersky Embedded Systems Security в конфигурации "Защита компьютера с помощью технологии "запрет по умолчанию" поверх версии программы, в которой используются сигнатурный анализ и антивирусные базы для защиты компьютера, набор компонентов программы будет автоматически сокращен за счет удаления следующих компонентов: • Постоянная защита файлов • Проверка по требованию • Компоненты, отвечающие за обновления Рекомендуется использовать эту конфигурацию для защиты систем с ограниченными ресурсами. В этом случае вы сможете активировать программу на длительный срок, а компонент Контроль запуска программ обеспечит защиту компьютера.
\product_long_term\ess_light.kud	Файл в формате Kaspersky Unicode Definition с описанием пакета установки для удаленной установки Kaspersky Embedded Systems Security через Kaspersky Security Center.
\product_long_term\klcfginst.exe	Программа установки Плагина управления Kaspersky Embedded Systems Security через Kaspersky Security Center. Установите Плагин управления на каждом защищаемом устройстве, на котором установлена Консоль администрирования Kaspersky Security Center, если вы планируете управлять Kaspersky Embedded Systems Security через нее.
\product_long_term\license.txt	Файл с текстом Лицензионного соглашения и Политики конфиденциальности.
\setup\setup.hta	Файл запуска программы приветствия.

Аппаратные и программные требования

Перед установкой Kaspersky Embedded Systems Security необходимо удалить с устройства другие антивирусные программы.

Программные требования к защищаемым устройствам

Вы можете установить Kaspersky Embedded Systems Security на компьютере под управлением 32-разрядной или 64-разрядной операционной системы Microsoft Windows.

Для установки и корректной работы программы на защищаемом устройстве под управлением операционной системы Windows XP требуется наличие установщика Windows версии 3.1.

Для установки и работы Kaspersky Embedded Systems Security на защищаемых устройствах со встроенными операционными системами необходим компонент Диспетчер фильтров (Filter Manager).

Вы можете установить Kaspersky Embedded Systems Security на устройство под управлением одной из следующих 32- или 64-разрядных операционных систем Microsoft Windows:

- Windows XP Embedded SP3 (32-разрядная);
- Windows Embedded POSReady 2009 (32-разрядная);
- Windows XP Professional SP2 / SP3 (32-разрядная, 64-разрядная);
- Windows Embedded Standard 7 SP1 (32-разрядная, 64-разрядная);
- Windows Embedded Enterprise 7 SP1 (32-разрядная, 64-разрядная);
- Windows Embedded POSReady 7 (32-разрядная, 64-разрядная);
- Windows 7 Professional / Enterprise SP1 (32-разрядная, 64-разрядная);
- Windows Embedded 8.1 Industry Professional / Enterprise (32-разрядная, 64-разрядная);
- Windows Embedded 8.0 Standard (32-разрядная, 64-разрядная);
- Windows 8 Professional / Enterprise (32-разрядная, 64-разрядная);
- Windows 8.1 Professional / Enterprise (32-разрядная, 64-разрядная);
- Windows 10 Professional / Enterprise (32-разрядная, 64-разрядная);
- Windows 10 IoT Enterprise (32-разрядная, 64-разрядная);
- Windows 10 Redstone 1 Professional / Enterprise / IoT Enterprise (32-разрядная, 64-разрядная);
- Windows 10 Redstone 2 Professional / Enterprise / IoT Enterprise (32-разрядная, 64-разрядная);
- Windows 10 Redstone 3 Professional / Enterprise / IoT Enterprise (32-разрядная, 64-разрядная);
- Windows 10 Redstone 4 Professional / Enterprise / IoT Enterprise (32-разрядная, 64-разрядная);

- Windows 10 Redstone 5 Professional / Enterprise / IoT Enterprise (32-разрядная, 64-разрядная);
- Windows 10 Redstone 6 Professional / Enterprise / IoT Enterprise (32-разрядная, 64-разрядная).

Аппаратные требования к защищаемым устройствам

Аппаратные требования к защищаемому устройству различаются в зависимости от версии операционной системы Windows.

- Аппаратные требования для устройств с операционными системами Windows XP (32 / 64-разрядная), Windows 7 (32-разрядная), Windows 8 (32-разрядная), Windows Embedded XP, Windows Embedded POSReady 2009 и Windows Embedded POSReady 7:
  - Минимальная конфигурация:
    - Объем дискового пространства:
      - для установки компонента Контроль запуска программ – 50 МБ;
      - для установки всех компонентов Kaspersky Embedded Systems Security – 2 ГБ.
    - Объем оперативной памяти:
      - 256 МБ для установки только компонента Контроль запуска программ на устройство с операционной системой Microsoft Windows;
      - 512 МБ для выполнения полной установки всех компонентов.
    - Требования к процессору:
      - для 32-разрядных операционных систем Microsoft Windows:
        1,4 ГГц, одноядерный;
        Intel® Pentium® III.
      - для 64-разрядных операционных систем Microsoft Windows:
        1,4 ГГц, одноядерный;
        Intel Pentium IV.
  - Рекомендуемая конфигурация:
    - Объем дискового пространства:
      - для установки компонента Контроль запуска программ – 2 ГБ;
      - для установки всех компонентов Kaspersky Embedded Systems Security – 4 ГБ.
    - Оперативная память: 2 ГБ.
    - Требования к процессору: 2,4 ГГц, четырехъядерный.
- Аппаратные требования для устройства с операционными системами Windows 7 (64-разрядная), Windows 8 (64-разрядная), Windows 10 (64-разрядная), Windows Embedded 7 и Windows Embedded 8:
  - Минимальная конфигурация:

- Объем дискового пространства:
  - для установки компонента Контроль запуска программ – 50 МБ;
  - для установки всех компонентов Kaspersky Embedded Systems Security – 2 ГБ.
- Оперативная память: 1 ГБ.
- Требования к процессору:
  - для 32-разрядных операционных систем Microsoft Windows:
    1,4 ГГц, одноядерный;
    Intel Pentium III.
  - для 64-разрядных операционных систем Microsoft Windows:
    1,4 ГГц, одноядерный;
    Intel Pentium IV.

- Рекомендуемая конфигурация:
  - Объем дискового пространства:
    - для установки компонента Контроль запуска программ – 2 ГБ;
    - для установки всех компонентов Kaspersky Embedded Systems Security – 4 ГБ.
  - Оперативная память: 2 ГБ.
  - Требования к процессору: 2,4 ГГц, четырехъядерный.

Функциональные требования и ограничения

В этом разделе приведено описание дополнительных функциональных требований и существующих ограничений компонентов Kaspersky Embedded Systems Security.

Установка и удаление

- Во время установки программы отображается предупреждение, если новый путь к папке установки Kaspersky Embedded Systems Security содержит более 150 символов. Это предупреждение не влияет на процесс установки. Программа Kaspersky Embedded Systems Security будет успешно установлена и запущена.
- Для установки компонентов, поддерживающих протокол SNMP, вам нужно перезапустить службу SNMP, если она запущена.
- Для установки и работы Kaspersky Embedded Systems Security на устройствах со встроенной операционной системой нужно установить компонент Диспетчер фильтров.
- Установка Средств администрирования Kaspersky Embedded Systems Security невозможна средствами групповых политик Microsoft Active Directory®.

- При установке программы на устройства с устаревшей версией операционной системы, для которой невозможно регулярное получение обновлений, нужно проверить следующие корневые сертификаты: DigiCert Assured ID Root CA, DigiCert_High_Assurance_EV_Root_CA, DigiCertAssuredIDRootCA. Если эти сертификаты отсутствуют, программа может работать некорректно. Рекомендуется установить указанные сертификаты любым возможным способом.

- Консоль Kaspersky Embedded Systems Security невозможно удалить из меню **Пуск**. Консоль Kaspersky Embedded Systems Security можно удалить с помощью ссылки в окне Установка / удаление программ.

Мониторинг файловых операций

По умолчанию компонент Мониторинг файловых операций не проверяет изменения в системных папках и в служебных файлах файловой системы, чтобы информация о стандартных изменениях файлов, постоянно осуществляемых операционной системой, не попадала в отчет выполнения задачи. Нельзя вручную добавить эти папки в область мониторинга.

Следующие папки и файлы исключены из области мониторинга:

- Служебные файлы NTFS с идентификатором файла от 0 до 33
- "%SystemRoot%\\Prefetch\\"
- "%SystemRoot%\\ServiceProfiles\\LocalService\\AppData\\Local\\"
- "%SystemRoot%\\System32\\LogFiles\\Scm\\"
- "%SystemRoot%\\Microsoft.NET\\Framework\\v4.0.30319\\"
- "%SystemRoot%\\Microsoft.NET\\Framework64\\v4.0.30319\\"
- "%SystemRoot%\\Microsoft.NET\\"
- "%SystemRoot%\\System32\\config\\"
- "%SystemRoot%\\Temp\\"
- "%SystemRoot%\\ServiceProfiles\\LocalService\\"
- "%SystemRoot%\\System32\\winevt\\Logs\\"
- "%SystemRoot%\\System32\\wbem\\repository\\"
- "%SystemRoot%\\System32\\wbem\\Logs\\"
- "%ProgramData%\\Microsoft\\Windows\\WER\\ReportQueue\\"
- "%SystemRoot%\\SoftwareDistribution\\DataStore\\"
- "%SystemRoot%\\SoftwareDistribution\\DataStore\\Logs\\"
- "%ProgramData%\\Microsoft\\Windows\\AppRepository\\"
- "%ProgramData%\\Microsoft\\Search\\Data\\Applications\\Windows\\"

- "%SystemRoot%\\Logs\\SystemRestore\\"
- "%SystemRoot%\\System32\\Tasks\\Microsoft\\Windows\\TaskScheduler\\"

Программа исключает папки верхнего уровня.

Компонент не осуществляет мониторинг изменений в файлах, которые происходят в обход файловой системы ReFS/NTFS (изменения, сделанные через BIOS, LiveCD и т.д.).

Управление сетевым экраном

- Работа с IP-адресами в формате IPv6 недоступна, если область указанного правила состоит из одного адреса.
- Текущие правила политики сетевого экрана поддерживают основные сценарии взаимодействия между защищаемыми устройствами и Сервером администрирования. Для использования функций Kaspersky Security Center в полном объеме нужно вручную настроить правила для портов. Информация о номерах портов, протоколах и их функциях приведена в Базе знаний Kaspersky Security Center (https://support.kaspersky.ru/ksc10, статья 9297).
- Программа не контролирует изменение правил и групп правил брандмауэра Windows во время выполнения задачи Управление сетевым экраном, если эти правила не добавлены в конфигурацию задачи при установке программы. Чтобы обновить статус и учитывать такие правила, нужно перезапустить задачу Управление сетевым экраном.
- При запуске задачи Управление сетевым экраном следующие типы правил автоматически удаляются из параметров сетевого экрана операционной системы:
  - запрещающие правила;
  - правила мониторинга исходящего трафика.

Установка и удаление программы

Этот раздел содержит пошаговые инструкции по установке и удалению Kaspersky Embedded Systems Security.

Коды программных компонентов Kaspersky Embedded Systems Security для службы установщика Windows

Файлы \product_long_term\ess_x86.msi и \product_long_term\ess_x64.msi предназначены для установки Kaspersky Embedded Systems Security в конфигурации **Защита компьютера с помощью технологии "запрет по умолчанию"**, а файлы \product\ess_x86.msi и \product\ess_x64.msi предназначены для установки Kaspersky Embedded Systems Security в конфигурации **Защита компьютера с помощью антивирусных баз**.

Если выбрана конфигурация "Защита компьютера с помощью антивирусных баз", все компоненты Kaspersky Embedded Systems Security, кроме компонентов Управление сетевым экраном и Счетчики производительности, включены по умолчанию.

При установке Kaspersky Embedded Systems Security в конфигурации "Защита компьютера с помощью антивирусных баз" поверх версии программы, в которой не используется сигнатурный анализ и антивирусные базы для защиты компьютера, набор компонентов программы будет автоматически расширен за счет добавления следующих компонентов:

- Постоянная защита файлов
- Проверка по требованию
- Защита от сетевых угроз

Компоненты, отвечающие за обновления, не входят в конфигурацию "Защита компьютера с помощью технологии "запрет по умолчанию".

Если выбрана конфигурация "Защита компьютера с помощью технологии "запрет по умолчанию", то по умолчанию включены следующие компоненты:

- Core
- Защита от эксплойтов
- Контроль запуска программ
- Значок области уведомлений

При установке Kaspersky Embedded Systems Security в конфигурации "Защита компьютера с помощью технологии "запрет по умолчанию" поверх версии программы, в которой используются сигнатурный анализ и антивирусные базы для защиты компьютера, набор компонентов программы будет автоматически сокращен за счет удаления следующих компонентов:

- Постоянная защита файлов
- Проверка по требованию
- Компоненты, отвечающие за обновления

Рекомендуется использовать эту конфигурацию для защиты систем с ограниченными ресурсами. В этом случае вы сможете активировать программу на длительный срок, а компонент Контроль запуска программ обеспечит защиту компьютера.

Файлы \console\esstools_x86.msi и \console\esstools_x64.msi устанавливают все программные компоненты набора Средства администрирования.

В следующих разделах приведены коды компонентов Kaspersky Embedded Systems Security для службы установщика Windows. Вы можете использовать эти коды, чтобы задать список устанавливаемых компонентов при установке Kaspersky Embedded Systems Security из командной строки.

Программные компоненты Kaspersky Embedded Systems Security

В следующей таблице приведены коды и описания программных компонентов Kaspersky Embedded Systems Security.

Описание программных компонентов Kaspersky Embedded Systems Security

Компонент	Идентификатор	Функции компонента
Основная функциональность	Core	Этот компонент включает в себя набор базовых функций программы и обеспечивает их работу.
Контроль запуска программ	AppCtrl	Этот компонент отслеживает попытки запуска программ пользователями и разрешает или запрещает запуск в соответствии с заданными правилами контроля запуска программ. Компонент реализуется в задаче Контроль запуска программ.
Контроль устройств	DevCtrl	Этот компонент отслеживает попытки подключения внешних

		устройств к защищаемому устройству и запрещает или разрешает их использование в соответствии с заданными правилами контроля устройств. Компонент реализуется в задаче Контроль устройств.
Антивирусная защита	AVProtection	Этот компонент обеспечивает антивирусную защиту и включает в себя следующие компоненты: • Проверка по требованию • Постоянная защита файлов
Защита от сетевых угроз	IDS	Этот компонент выполняет проверку входящего сетевого трафика на наличие активности, характерной для сетевых атак. При обнаружении попытки сетевой атаки, нацеленной на ваш компьютер, Kaspersky Security для Windows Server блокирует сетевую активность со стороны атакующего компьютера.
Проверка по требованию	Ods	Этот компонент устанавливает системные файлы Kaspersky Embedded Systems Security и выполняет задачи проверки по требованию (проверка объектов защищаемого устройства, выполняемая по команде). Если, устанавливая Kaspersky Embedded Systems Security из командной строки, вы укажете другие компоненты Kaspersky Embedded Systems Security, не указывая компонент Core, компонент Core будет установлен автоматически.
Постоянная защита файлов	Oas	Этот компонент выполняет антивирусную проверку файлов на защищаемом устройстве при обращении к этим файлам. Компонент реализует задачу Постоянная защита файлов.
Использование Kaspersky Security Network	Ksn	Этот компонент обеспечивает защиту на основе облачных технологий "Лаборатории Касперского". Компонент реализует задачу Использование KSN (отправка запросов и получение заключений от службы Kaspersky Security Network).
Мониторинг файловых операций	Fim	Этот компонент позволяет регистрировать операции, производимые над файлами в выбранной области мониторинга. Компонент реализует задачу Мониторинг файловых операций.
Защита от эксплойтов	AntiExploit	Этот компонент обеспечивает управление параметрами защиты процессов в памяти устройства.
Управление сетевым экраном	Firewall	Этот компонент предоставляет возможность управления брандмауэром Windows через графический интерфейс Kaspersky Embedded Systems Security. Компонент реализует задачу Управление сетевым экраном.
Модуль интеграции с Агентом администрирования Kaspersky Security Center	AKIntegration	Этот компонент обеспечивает связь Kaspersky Embedded Systems Security с Агентом администрирования Kaspersky Security Center. Вы можете установить этот компонент на защищаемом устройстве, если вы планируете управлять программой через Kaspersky Security Center.
Анализ журналов	LogInspector	Компонент выполняет контроль целостности защищаемой

		среды на основе результатов анализа журналов событий Windows.
Набор счетчиков производительности программы Системный монитор	PerfMonCounters	Компонент устанавливает набор счетчиков производительности программы Системный монитор. Счетчики производительности позволяют измерять производительность Kaspersky Embedded Systems Security и находить возможные узкие места при совместной работе Kaspersky Embedded Systems Security с другими программами.
Поддержка SNMP-протокола	SnmpSupport	Компонент публикует счетчики и ловушки Kaspersky Embedded Systems Security через Simple Network Management Protocol (протокол SNMP) в Microsoft Windows. Этот компонент можно установить на защищаемое устройство, только если на нем уже установлена служба SNMP.
Значок Kaspersky Embedded Systems Security в области уведомлений	TrayApp	Компонент отображает значок Kaspersky Embedded Systems Security в области уведомлений панели задач защищаемого устройства. Значок Kaspersky Embedded Systems Security показывает состояние защиты устройства и позволяет открыть Консоль программы с помощью Microsoft Management Console, если она установлена, и окно **О программе**.

Программные компоненты набора Средства администрирования

В следующей таблице приведены коды и описание программных компонентов набора Средства администрирования.

Описание программных компонентов набора Средства администрирования

Компонент	Код	Функции компонента
Оснастка Kaspersky Embedded Systems Security	MmcSnapin	Компонент устанавливает оснастку Microsoft Management Console для управления через Консоль Kaspersky Embedded Systems Security. Если при установке набора "Средства администрирования" из командной строки, вы укажете другие компоненты набора, но не укажите компонент MmcSnapin, компонент MmcSnapin будет установлен автоматически.
Документация	Help	Kaspersky Embedded Systems Security добавляет ярлык для перехода на веб-сайт "Лаборатории Касперского", где документ "Руководство администратора" доступен в формате онлайн-справки. Этот ярлык доступен из меню **Пуск**.

Изменения в системе после установки Kaspersky Embedded Systems Security

При совместной установке Kaspersky Embedded Systems Security и набора "Средства администрирования", включающего Консоль программы, служба установщика Windows выполняет на защищаемом устройстве следующие изменения:

- создает папки Kaspersky Embedded Systems Security на защищаемом устройстве и на защищаемом устройстве, на котором установлена Консоль программы;

- регистрирует службы Kaspersky Embedded Systems Security;
- создает группу пользователей Kaspersky Embedded Systems Security;
- регистрирует в системном реестре ключи Kaspersky Embedded Systems Security.

Эти изменения описаны ниже.

Папки Kaspersky Embedded Systems Security на защищаемом устройстве

При установке Kaspersky Embedded Systems Security на защищаемом устройстве создаются следующие папки:

- Заданная по умолчанию папка установки Kaspersky Embedded Systems Security, содержащая исполняемые файлы Kaspersky Embedded Systems Security в зависимости от разрядности операционной системы. По умолчанию используются следующие папки установки:
  - В 32-х разрядной версии Microsoft Windows: %ProgramFiles%\Kaspersky Lab\Kaspersky Embedded Systems Security\
  - В 64-х разрядной версии Microsoft Windows: %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Embedded Systems Security\
- Файлы Management Information Base (MIB), содержащие описание счетчиков и ловушек, публикуемых Kaspersky Embedded Systems Security по протоколу SNMP.
  - %Kaspersky Embedded Systems Security%\mibs
- 64-разрядные версии исполняемых файлов Kaspersky Embedded Systems Security (папка создается только при установке Kaspersky Embedded Systems Security в 64-разрядной версии Microsoft Windows).
  - %Kaspersky Embedded Systems Security%\x64
- Служебные файлы Kaspersky Embedded Systems Security:
  - %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\3.0\Data\
  - %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\3.0\Settings\
  - %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\3.0\Dskm\

  Для Windows XP путь к папке Kaspersky Lab – %ALLUSERSPROFILE%\Application Data\.
- Файлы с параметрами источников обновлений:

  %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\3.0\Update\

  %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\3.0\Update\
- Обновления баз и программных модулей, загруженные с помощью задачи Копирование обновлений (папка создается при первой загрузке обновлений с помощью задачи Копирование обновлений).

  %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\3.0\Update\Distribution\
- Журналы выполнения задач и журнал системного аудита.

%ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\3.0\Reports\

- Набор используемых баз данных.

  %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\3.0\Bases\Current\

- Резервные копии баз; перезаписываются при каждом обновлении баз.

  %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\3.0\Bases\Backup\

- Временные файлы, создаваемые при выполнении задач обновления.

  %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\3.0\Bases\Temp\

- Объекты на карантине (папка по умолчанию).

  %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\3.0\Quarantine\

- Объекты в резервном хранилище (папка по умолчанию).

  %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\3.0\Backup\

- Объекты, восстановленные из резервного хранилища и карантина (папка по умолчанию для восстановленных объектов).

  %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\3.0\Restored\

Папка, создаваемая при установке Консоли программы

Заданная по умолчанию папка установки Консоли программы, содержащая файлы набора "Средства администрирования", зависит от разрядности операционной системы. По умолчанию используются следующие папки установки:

- В 32-х разрядной версии Microsoft Windows: %ProgramFiles%\Kaspersky Lab\Kaspersky Embedded Systems Security Admins Tools\
- В 64-х разрядной версии Microsoft Windows: %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Embedded Systems Security Admins Tools\

Службы Kaspersky Embedded Systems Security

Следующие службы Kaspersky Embedded Systems Security запускаются под системной учетной записью Локальная система (SYSTEM).

- Kaspersky Security Service (KAVFS) – это основная служба Kaspersky Embedded Systems Security, которая управляет задачами и рабочими процессами Kaspersky Embedded Systems Security.
- Служба Kaspersky Security Management (KAVFSGT) – это служба, предназначенная для управления Kaspersky Embedded Systems Security через Консоль программы.
- Служба Kaspersky Security Exploit Prevention (KAVFSSLP) – это служба, исполняющая роль посредника при передаче параметров безопасности внешним агентам безопасности и при получении данных о событиях безопасности.

Группа Kaspersky Embedded Systems Security

ESS Administrators – это группа на защищаемом устройстве, пользователи которой имеют полный доступ к службе Kaspersky Security Management и ко всем функциям Kaspersky Embedded Systems Security.

Ключи системного реестра

При установке Kaspersky Embedded Systems Security создаются следующие ключи системного реестра:

- Свойства Kaspersky Embedded Systems Security:
  [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\KAVFS]
- Параметры журнала событий Kaspersky Embedded Systems Security (Kaspersky Event Log):
  [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Kaspersky Security]
- Свойства службы управления Kaspersky Embedded Systems Security:
  [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\KAVFSGT]
- Параметры счетчиков производительности:
  - В 32-х разрядной версии Microsoft Windows:
    [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Kaspersky Security\Performance]
  - В 64-х разрядной версии Microsoft Windows:
    [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Kaspersky Security x64\Performance]
- Параметры компонента Поддержка SNMP-протокола:
  - В 32-х разрядной версии Microsoft Windows:
    [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\ESS\3.0\SnmpAgent]
  - В 64-х разрядной версии Microsoft Windows:
    [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\ESS\3.0\SnmpAgent]
- Параметры файла дампа:
  - В 32-х разрядной версии Microsoft Windows:
    [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\ESS\3.0\CrashDump]
  - В 64-х разрядной версии Microsoft Windows:
    [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\ESS\3.0\CrashDump]
- Параметры файла трассировки:
  - В 32-х разрядной версии Microsoft Windows:
    [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\ESS\3.0\Trace]
  - В 64-х разрядной версии Microsoft Windows:
    [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\ESS\3.0\Trace]
- Параметры задач и функций программы:
  [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\ESS\3.0\Environment]

Процессы Kaspersky Embedded Systems Security

Kaspersky Embedded Systems Security запускает процессы, описанные в таблице ниже.

Процессы Kaspersky Embedded Systems Security

Имя файла	Назначение
kavfswp.exe	Рабочий процесс Kaspersky Embedded Systems Security
kavtray.exe	Процесс значка области уведомлений
kavfsmui.exe	Процесс компонента Диагностическое окно
kavshell.exe	Процесс утилиты командной строки
kavfsrcn.exe	Процесс удаленного управления Kaspersky Embedded Systems Security
kavfs.exe	Процесс службы Kaspersky Security
kavfsgt.exe	Процесс службы Kaspersky Security Management
kavfswh.exe	Процесс службы Kaspersky Security Exploit Prevention

Параметры установки и удаления и ключи командной строки для службы установщика Windows

В этом разделе описаны параметры установки и удаления Kaspersky Embedded Systems Security, их значения по умолчанию, указаны ключи для изменения параметров установки и возможные значения этих ключей. Вы можете использовать эти ключи вместе со стандартными ключами команды `msiexec` службы установщика Windows при установке Kaspersky Embedded Systems Security из командной строки.

Параметры установки и ключи командной строки для установщика Windows

- Согласие с условиями Лицензионного соглашения: необходимо принять условия для установки Kaspersky Embedded Systems Security.

  Возможны следующие значения ключа командной строки `EULA=<значение>`:

  - `0` – вы отклоняете условия Лицензионного соглашения (значение по умолчанию).
  - `1` – вы принимаете условия Лицензионного соглашения.

- Согласие с условиями Политики конфиденциальности: необходимо принять условия для установки Kaspersky Embedded Systems Security.

  Возможны следующие значения ключа командной строки `PRIVACYPOLICY=<значение>`:

  - `0` – вы отклоняете условия Политики конфиденциальности (значение по умолчанию).
  - `1` – вы принимаете условия Политики конфиденциальности.

- Разрешить установку Kaspersky Embedded Systems Security, если не установлено обновление KB4528760. Дополнительная информация об обновлении KB4528760 приведена на веб-сайте Microsoft.

  Возможны следующие значения ключа командной строки `PRIVACYPOLICY=<значение>`:

  - `0` – отменить установку Kaspersky Embedded Systems Security, если не установлено обновление KB4528760 (значение по умолчанию).

- `1` – разрешить установку Kaspersky Embedded Systems Security, если не установлено обновление KB4528760.

  Обновление KB4528760 исправляет уязвимость безопасности CVE-2020-0601. Дополнительная информация об уязвимости в системе безопасности CVE-2020-0601 приведена на веб-сайте Microsoft.

- Установка Kaspersky Embedded Systems Security с предварительной проверкой активных процессов и загрузочных секторов локальных дисков.

  Возможны следующие значения ключа командной строки `PRESCAN=<значение>`:

  - `0` – не выполнять предварительную проверку активных процессов и загрузочных секторов локальных дисков во время установки (значение по умолчанию).
  - `1` – выполнить предварительную проверку активных процессов и загрузочных секторов локальных дисков во время установки.

- Папка, в которую будут сохранены файлы Kaspersky Embedded Systems Security при установке. Вы можете указать другую папку.

  Значение по умолчанию для ключа командной строки `INSTALLDIR=<полный путь к папке>`:

  - Kaspersky Embedded Systems Security: %ProgramFiles%\Kaspersky Lab\Kaspersky Embedded Systems Security
  - Средства администрирования: %ProgramFiles%\Kaspersky Lab\Kaspersky Embedded Systems Security Admins Tools
  - В Microsoft Windows 64-разрядной версии: %ProgramFiles(x86)%

- Задача Постоянная защита файлов запускается сразу после запуска Kaspersky Embedded Systems Security. Включите этот параметр, чтобы запустить Постоянную защиту файлов при запуске Kaspersky Embedded Systems Security (рекомендуется).

  Возможны следующие значения ключа командной строки `RUNRTP=<значение>`:

  - `1` – запустить (значение по умолчанию).
  - `0` – не запускать.

- Исключения из области защиты, рекомендуемые корпорацией Microsoft. В задаче Постоянная защита файлов исключите из области защиты объекты на устройстве, которые рекомендует исключать корпорация Microsoft. Некоторые программы на защищаемом устройстве могут работать нестабильно, когда антивирусная программа перехватывает или изменяет файлы, используемые этими программами. К таким программам корпорация Microsoft относит, например, некоторые программы контроллеров доменов.

  Возможны следующие значения ключа командной строки `ADDMSEXCLUSION=<значение>`:

  - `1` – исключить (значение по умолчанию).
  - `0` – не исключать.

- Объекты, исключаемые из области защиты в соответствии с рекомендациями "Лаборатории Касперского". В задаче Постоянная защита файлов исключите из области защиты объекты на устройстве, которые рекомендует исключать "Лаборатория Касперского".

  Возможны следующие значения ключа командной строки `ADDKLEXCLUSION=<значение>`:

- `1` – исключить (значение по умолчанию).
- `0` – не исключать.

- Разрешить удаленное подключение к Консоли программы По умолчанию удаленное подключение к Консоли программы, установленной на защищаемом устройстве, не разрешено. Во время установки можно разрешить подключение. Kaspersky Embedded Systems Security создаст разрешающие правила для процесса kavfsgt.exe по протоколу TCP для всех портов.

  Возможны следующие значения ключа командной строки `ALLOWREMOTECON=<значение>`:

  - `1` – разрешить.
  - `0` – запретить (значение по умолчанию).

- Путь к файлу ключа (`LICENSEKEYPATH`)

  . По умолчанию установщик Windows пытается найти файл с расширением .key в папке \product комплекта поставки. Если в папке \product имеется несколько файлов ключа, установщик Windows выбирает файл ключа с самой поздней датой истечения срока действия. Можно предварительно сохранить файл ключа в папке \product или указать другой путь к файлу ключа с помощью параметра **Добавить ключ**. Вы можете добавить ключ после установки Kaspersky Embedded Systems Security с помощью выбранного вами средства администрирования, например, через Консоль программы. Если вы не добавите ключ во время установки программы, после установки Kaspersky Embedded Systems Security не будет функционировать.

- Путь к конфигурационному файлу. Kaspersky Embedded Systems Security импортирует параметры из указанного конфигурационного файла, созданного в программе. Kaspersky Embedded Systems Security не импортирует из конфигурационного файла пароли, например пароли учетных записей для запуска задач или пароли для соединения с прокси-сервером. После импорта параметров вам нужно ввести все пароли вручную. Если вы не укажете конфигурационный файл, после установки программа начнет работать с параметрами по умолчанию.

  Значение по умолчанию для параметра `CONFIGPATH=<имя конфигурационного файла>` не указано.

- Параметр включения сетевых соединений для Консоли программы используется для установки Консоли Kaspersky Embedded Systems Security на другое устройство. Вы можете удаленно управлять защитой устройства с другого устройства, на котором установлена Консоль Kaspersky Embedded Systems Security. В брандмауэре Microsoft Windows будет открыт TCP-порт 135, разрешены сетевые соединения для исполняемого файла kavfsrcn.exe для удаленного управления Kaspersky Embedded Systems Security и предоставлен доступ к DCOM-программам. После завершения установки добавьте пользователей в группу ESS Administrators, чтобы разрешить им управлять программой удаленно, а также разрешите на защищаемом устройстве сетевые подключения к службе Kaspersky Security Management (файл kavfsgt.exe). Можно более детально ознакомиться с дополнительной настройкой при установке Консоли Kaspersky Embedded Systems Security на другое устройство.

  Возможны следующие значения ключа командной строки `ADDWFEXCLUSION=<значение>`:

  - `1` – разрешить.
  - `0` – запретить (значение по умолчанию).

- Отключение проверки на наличие несовместимого программного обеспечения. Используйте этот параметр, чтобы включить или выключить проверку на наличие несовместимого программного обеспечения при установке программы на защищаемое устройство в фоновом режиме. Независимо от значения этого параметра, при установке Kaspersky Embedded Systems Security программа всегда предупреждает о других версиях программы, установленных на этом защищаемом устройстве.

  Возможны следующие значения ключа командной строки `SKIPINCOMPATIBLESW=<значение>`:

- `0` – выполняется проверка на несовместимое программное обеспечение (значение по умолчанию).
- `1` – проверка на наличие несовместимого программного обеспечения не выполняется.

Параметры удаления и ключи командной строки для установщика Windows

- Восстановление содержимого карантина.

  Возможны следующие значения ключа командной строки `RESTOREQTN=<значение>`:

  - `0` – удалить содержимое карантина (значение по умолчанию).
  - `1` – восстановить содержимое карантина в папку, указанную в качестве значения параметра RESTOREPATH, во вложенную подпапку \Quarantine.

- Восстановление содержимого резервного хранилища.

  Возможны следующие значения ключа командной строки `RESTOREBCK=<значение>`:

  - `0` – удалить содержимое резервного хранилища (значение по умолчанию).
  - `1` – восстановить содержимое резервного хранилища в папку, указанную в качестве значения параметра RESTOREPATH, во вложенную папку \Backup.

- Ввод текущего пароля для подтверждения операции удаления (при включенной функции защиты паролем).

  Значение по умолчанию для ключа `UNLOCK_PASSWORD=<указанный пароль>` не задано.

- Папка для восстановленных объектов. Восстановленные объекты будут сохранены в указанной папке.

  Значение по умолчанию для ключа командной строки `RESTOREPATH=<полный путь к папке>` – %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\3.0\Restored.

Журналы установки и удаления Kaspersky Embedded Systems Security

Если вы выполняете установку или удаление Kaspersky Embedded Systems Security с помощью мастера установки (удаления), служба установщика Windows создает журнал установки (удаления). Файл журнала с именем ess_v3.0_install_<uid>.log (где <uid> – это уникальный восьмизначный идентификатор журнала) сохраняется в папку %temp% пользователя, с правами учетной записи которого был запущен файл setup.exe.

Если в меню **Пуск** вы выбрали пункт **Изменение или удаление Средств администрирования Kaspersky Embedded Systems Security** для Консоли программы или для Kaspersky Embedded Systems Security, в папке %temp% будет автоматически создан файл журнала с именем ess_3.0_maintenance.log.

Если вы выполняете установку или удаление Kaspersky Embedded Systems Security из командной строки, по умолчанию файл журнала установки не создается.

Чтобы установить Kaspersky Embedded Systems Security и создать файл журнала на диске C:\, выполните одну из следующих команд:

- `msiexec /i ess_x86.msi /l*v C:\ess.log /qn EULA=1 PRIVACYPOLICY=1`
- `msiexec /i ess_x64.msi /l*v C:\ess.log /qn EULA=1 PRIVACYPOLICY=1`

Планирование установки

В этом разделе описаны средства администрирования Kaspersky Embedded Systems Security, особенности установки и удаления Kaspersky Embedded Systems Security с помощью мастера установки, из командной строки, с помощью Kaspersky Security Center и через групповые политики Active Directory.

Перед началом установки Kaspersky Embedded Systems Security составьте план основных этапов установки.

1. Выберите средства администрирования, которые вы будете использовать для управления Kaspersky Embedded Systems Security и для настройки программы.
2. Определите, какие программные компоненты требуется установить.
3. Выберите способ установки.

Выбор средств администрирования

Определите, какие средства администрирования вы будете использовать для настройки параметров и управления Kaspersky Embedded Systems Security. В качестве средств администрирования Kaspersky Embedded Systems Security вы можете использовать Консоль программы, утилиту командной строки и Консоль администрирования Kaspersky Security Center.

Консоль Kaspersky Embedded Systems Security

Консоль Kaspersky Embedded Systems Security представляет собой самостоятельную оснастку, которая добавляется в Microsoft Management Console. Вы можете управлять Kaspersky Embedded Systems Security через Консоль программы, установленную на защищаемом устройстве или на другом устройстве в сети организации.

Вы можете добавить несколько оснасток Kaspersky Embedded Systems Security в Microsoft Management Console в авторском режиме, чтобы управлять защитой нескольких устройств, на которых установлена программа Kaspersky Embedded Systems Security.

Консоль программы входит в набор компонентов "Средства администрирования".

Утилита командной строки

Вы можете управлять Kaspersky Embedded Systems Security из командной строки защищаемого устройства.

Утилита командной строки входит в набор программных компонентов Kaspersky Embedded Systems Security.

Kaspersky Security Center

Если вы используете Kaspersky Security Center для централизованного управления антивирусной защитой устройств в вашей организации, вы можете управлять Kaspersky Embedded Systems Security через Консоль администрирования Kaspersky Security Center.

Вам потребуется установить следующие компоненты:

- **Модуль интеграции с Агентом администрирования Kaspersky Security Center**. Этот компонент входит в группу программных компонентов Kaspersky Embedded Systems Security. Он позволяет Kaspersky Embedded Systems Security взаимодействовать с Агентом администрирования. Установите модуль интеграции с Агентом администрирования Kaspersky Security Center на защищаемое устройство.

- **Агент администрирования Kaspersky Security Center**. Установите его на каждое защищаемое устройство. Этот компонент будет обеспечивать взаимодействие между программой Kaspersky Embedded Systems Security, установленной на защищаемом устройстве, и Консолью администрирования Kaspersky Security Center. Файл установки Агента администрирования входит в комплект поставки Kaspersky Security Center.

- **Плагин управления Kaspersky Embedded Systems Security**. Дополнительно на управляемом устройстве, на котором установлен Сервер администрирования Kaspersky Security Center, установите Плагин управления Kaspersky Embedded Systems Security для работы через Консоль администрирования. Плагин обеспечивает интерфейс управления программой через Kaspersky Security Center. Файл установки Плагина управления \product\klcfginst.exe входит в комплект поставки Kaspersky Embedded Systems Security.

Выбор способа установки

После определения программных компонентов для установки Kaspersky Embedded Systems Security, вам нужно выбрать способ установки программы.

Выберите способ установки в зависимости от архитектуры сети и следующих условий:

- Потребуется ли вам задать специальные параметры установки Kaspersky Embedded Systems Security или вы будете использовать рекомендуемые параметры установки.

- Будут ли параметры установки едиными для всех защищаемых устройств или индивидуальными для каждого защищаемого устройства.

Вы можете установить Kaspersky Embedded Systems Security как с помощью мастера установки, так и в режиме без взаимодействия с пользователем, указав параметры установки в командной строке. Вы можете выполнить централизованную удаленную установку Kaspersky Embedded Systems Security: через групповые политики Active Directory или с помощью задачи удаленной установки Kaspersky Security Center.

Вы можете установить и настроить Kaspersky Embedded Systems Security на отдельном защищаемом устройстве и сохранить его параметры в конфигурационный файл, чтобы затем использовать созданный файл для установки Kaspersky Embedded Systems Security на другие защищаемые устройства. Однако это невозможно при установке программы через групповые политики Active Directory.

Запуск мастера установки

С помощью мастера установки вы можете установить:

- Компоненты Kaspersky Embedded Systems Security из файла \product\setup.exe, входящего в комплект поставки, на защищаемом устройстве.

- Консоль Kaspersky Embedded Systems Security из файла \console\setup.exe, входящего в комплект поставки, на защищаемом устройстве или другом устройстве в локальной сети.

Запуск из командной строки файла пакета установки с параметрами установки

Запустив файл пакета установки без ключей, вы установите Kaspersky Embedded Systems Security с параметрами установки по умолчанию. С помощью ключей Kaspersky Embedded Systems Security вы можете изменять параметры установки.

Вы можете установить Консоль программы на защищаемом устройстве или на рабочем месте администратора.

Вы также можете использовать команды для установки Kaspersky Embedded Systems Security и Консоли программы.

Централизованная установка через Kaspersky Security Center

Если вы используете Kaspersky Security Center для управления антивирусной защитой устройств в сети, вы можете установить Kaspersky Embedded Systems Security на несколько устройств с помощью задачи удаленной установки.

Защищаемые устройства, на которых вы хотите установить Kaspersky Embedded Systems Security с помощью Kaspersky Security Center, могут находиться как в одном домене с Kaspersky Security Center, так и в другом домене, а также вообще не принадлежать ни к одному домену.

Централизованная установка через групповые политики Active Directory

С помощью групповых политик Active Directory вы можете устанавливать Kaspersky Embedded Systems Security на защищаемом устройстве. Вы можете установить Консоль программы на защищаемом устройстве или рабочем месте администратора.

Вы можете установить Kaspersky Embedded Systems Security, используя только параметры установки по умолчанию.

Защищаемые устройства, на которых программа Kaspersky Embedded Systems Security была установлена с помощью групповых политик Active Directory, должны находиться в том же домене и в том же подразделении организации. Установка выполняется при запуске защищаемого устройства, перед входом в Microsoft Windows.

Установка и удаление программы с помощью мастера

В этом разделе описана установка и удаление Kaspersky Embedded Systems Security и Консоли программы с помощью мастера установки, а также приведена информация о дополнительных параметрах Kaspersky Embedded Systems Security и действиях при установке.

Установка с помощью мастера установки

В следующих разделах содержится информация об установке Kaspersky Embedded Systems Security и Консоли программы.

Чтобы установить и начать использовать Kaspersky Embedded Systems Security, выполните следующие действия:

1. Установите Kaspersky Embedded Systems Security на защищаемое устройство.

2. На устройства, с которых вы планируете управлять Kaspersky Embedded Systems Security, установите Консоль программы.

3. Если вы установили Консоль программы не на защищаемом устройстве, а на другом устройстве сети, выполните дополнительную настройку, чтобы пользователи Консоли программы могли удаленно управлять Kaspersky Embedded Systems Security.

4. Выполните действия после установки Kaspersky Embedded Systems Security.

Установка Kaspersky Embedded Systems Security

Перед установкой Kaspersky Embedded Systems Security выполните следующие действия:

Убедитесь, что на защищаемом устройстве не установлены другие антивирусные программы.

- Убедитесь, что учетная запись, с правами которой вы запускаете мастер установки, входит в группу администраторов на защищаемом устройстве.

После выполнения описанных выше действий, перейдите к процедуре установки. Следуя инструкциям мастера установки, задайте параметры установки Kaspersky Embedded Systems Security. Вы можете прервать установку Kaspersky Embedded Systems Security на любом шаге мастера установки. Для этого в окне мастера установки нажмите на кнопку **Отмена**.

Можно более детально ознакомиться с параметрами установки (удаления).

Чтобы установить Kaspersky Embedded Systems Security с помощью мастера установки, выполните следующие действия:

1. На защищаемом устройстве запустите файл setup.exe.

2. В открывшемся окне в разделе **Установка** перейдите по ссылке **Установить защиту на основе белых списков** или **Установить защиту на основе антивирусных баз**.

   Если выбрана конфигурация "Защита компьютера с помощью антивирусных баз", все компоненты Kaspersky Embedded Systems Security, кроме компонентов Управление сетевым экраном и Счетчики производительности, включены по умолчанию.

   При установке Kaspersky Embedded Systems Security в конфигурации "Защита компьютера с помощью антивирусных баз" поверх версии программы, в которой не используется сигнатурный анализ и антивирусные базы для защиты компьютера, набор компонентов программы будет автоматически расширен за счет добавления следующих компонентов:

   - Постоянная защита файлов
   - Проверка по требованию
   - Защита от сетевых угроз

Компоненты, отвечающие за обновления, не входят в конфигурацию "Защита компьютера с помощью технологии "запрет по умолчанию".

Если выбрана конфигурация "Защита компьютера с помощью технологии "запрет по умолчанию", то по умолчанию включены следующие компоненты:

- Core
- Защита от эксплойтов
- Контроль запуска программ
- Значок области уведомлений

При установке Kaspersky Embedded Systems Security в конфигурации "Защита компьютера с помощью технологии "запрет по умолчанию" поверх версии программы, в которой используются сигнатурный анализ и антивирусные базы для защиты компьютера, набор компонентов программы будет автоматически сокращен за счет удаления следующих компонентов:

- Постоянная защита файлов
- Проверка по требованию
- Компоненты, отвечающие за обновления

Рекомендуется использовать эту конфигурацию для защиты систем с ограниченными ресурсами. В этом случае вы сможете активировать программу на длительный срок, а компонент Контроль запуска программ обеспечит защиту компьютера.

3. В открывшемся окне приветствия мастера установки Kaspersky Embedded Systems Security нажмите на кнопку **Далее**.

   Откроется окно **Лицензионное соглашение и Политика конфиденциальности**.

4. Ознакомьтесь с условиями Лицензионного соглашения и Политики конфиденциальности.

5. Если вы согласны с условиями и положениями Лицензионного соглашения и Политики конфиденциальности, для продолжения установки установите флажки **Я подтверждаю, что полностью прочитал, понимаю и принимаю положения и условия настоящего Лицензионного соглашения** и **Я понимаю и соглашаюсь, что мои данные будут обрабатываться и пересылаться (в том числе в третьи страны), согласно «Политике конфиденциальности». Я подтверждаю, что полностью прочитал и понимаю «Политику конфиденциальности»**.

   Если вы не принимаете Лицензионное соглашение и Политику конфиденциальности, установка будет прервана.

6. Нажмите на кнопку **Далее**.

   Откроется окно **Быстрая проверка устройства перед началом установки**.

7. В окне **Быстрая проверка устройства перед началом установки** установите флажок **Проверить устройство на вирусы**, чтобы проверить на наличие угроз системную память и загрузочные секторы локальных дисков защищаемого устройства. Нажмите на кнопку **Далее**. По окончании проверки откроется окно с результатами проверки.

В окне содержится информация о проверенных объектах на управляемом устройстве: общее количество проверенных объектов, количество обнаруженных угроз, количество обнаруженных зараженных и возможно зараженных объектов, количество опасных или подозрительных процессов, которые программа Kaspersky Embedded Systems Security удалила из памяти, и количество опасных или подозрительных процессов, которые программе не удалось удалить.

Чтобы посмотреть, какие именно объекты были проверены, нажмите на кнопку **Список обработанных объектов**.

8. В окне **Быстрая проверка устройства перед началом установки** нажмите на кнопку **Далее**.

   Откроется окно **Выборочная установка**.

9. Выберите компоненты, которые вы хотите установить.

   Компонент Поддержка SNMP-протокола Kaspersky Embedded Systems Security отображается в списке устанавливаемых компонентов, только если на защищаемом устройстве установлена служба Microsoft Windows SNMP.

10. Чтобы отменить все изменения, в окне **Выборочная установка** нажмите на кнопку **Сбросить**. Нажмите на кнопку **Далее**.

11. В окне **Выбор папки назначения** выполните следующие действия:

    - Если требуется, укажите папку, в которой будут сохранены файлы Kaspersky Embedded Systems Security.
    - Если требуется, нажмите на кнопку **Диск** для просмотра информации о доступном пространстве на локальных жестких дисках.

    Нажмите на кнопку **Далее**.

12. В окне **Дополнительные параметры установки** настройте следующие параметры установки:

    - **Включить постоянную защиту после установки программы**
    - **Добавить к исключениям файлы, рекомендованные Microsoft**
    - **Добавить к исключениям файлы, рекомендованные "Лабораторией Касперского"**

      Нажмите на кнопку **Далее**.

13. В окне **Импорт параметров из конфигурационного файла** выполните следующие действия:

    a. Если вы хотите импортировать параметры Kaspersky Embedded Systems Security из существующего конфигурационного файла, созданного в любой предыдущей совместимой версии программы, укажите конфигурационный файл.

    b. Нажмите на кнопку **Далее**.

14. В окне **Активация программы** выполните одно из следующих действий:

    - Если вы хотите активировать программу, укажите файл ключа Kaspersky Embedded Systems Security для активации программы.
    - Если вы хотите активировать программу позже, нажмите на кнопку **Далее**.

- Если вы предварительно сохранили файл ключа в папке \product комплекта поставки, имя этого файла отобразится в поле **Ключ**.

  Чтобы добавить ключ с помощью файла ключа, который хранится в другой папке, укажите файл ключа.

  После добавления файла ключа в окне отобразится информация о лицензии. В Kaspersky Embedded Systems Security отображается расчетная дата истечения срока действия лицензии. Срок действия лицензии отсчитывается с момента добавления ключа, а истекает не позднее даты окончания срока действия файла ключа.

  Нажмите на кнопку **Далее**, чтобы добавить файл ключа в программу.

15. В окне **Готовность к установке** нажмите на кнопку **Установить**. Мастер приступит к установке компонентов Kaspersky Embedded Systems Security.

16. По завершении установки откроется окно **Установка завершена**.

17. Установите флажок **Прочитать информацию о релизе**, чтобы просмотреть информацию о версии после завершения работы мастера установки.

18. Нажмите на кнопку **Готово**.

Работа мастера установки будет завершена. По завершении установки программа Kaspersky Embedded Systems Security готова к работе, если вы добавили ключ активации.

Установка Консоли Kaspersky Embedded Systems Security

Следуя инструкциям мастера установки, настройте параметры установки Консоли программы. Вы можете прервать установку на любом шаге мастера. Для этого в окне мастера установки нажмите на кнопку **Отмена**.

Чтобы установить Консоль программы, выполните следующие действия:

1. Убедитесь, что учетная запись, с правами которой вы запускаете мастер установки, входит в группу администраторов на устройстве.

2. На защищаемом устройстве запустите файл setup.exe.

   Откроется окно программы-приветствия.

3. Перейдите по ссылке **Установить Консоль Kaspersky Embedded Systems Security**.

   Откроется окно приветствия мастера установки.

4. Нажмите на кнопку **Далее**.

5. В открывшемся окне ознакомьтесь с условиями Лицензионного соглашения и Политики конфиденциальности и, чтобы продолжить установку, установите флажки под заголовком **Я подтверждаю, что полностью прочитал, понимаю и принимаю положения и условия настоящего Лицензионного соглашения**.

6. Нажмите на кнопку **Далее**.

   Откроется окно **Дополнительные параметры установки**.

7. В окне **Дополнительные параметры установки** выполните следующие действия:

- Если вы планируете с помощью Консоли программы управлять программой Kaspersky Embedded Systems Security, установленной на удаленном устройстве, установите флажок **Разрешить удаленный доступ**.

- Чтобы открыть окно **Выборочная установка** и выбрать компоненты, выполните следующие действия:

  a. Нажмите на кнопку **Дополнительно**.

  Откроется окно **Выборочная установка**.

  b. В списке выберите набор компонентов "Средства администрирования".

  По умолчанию устанавливаются все компоненты.

  c. Нажмите на кнопку **Далее**.

Можно ознакомиться с более подробной информацией о компонентах Kaspersky Embedded Systems Security.

8. В окне **Выбор папки назначения** выполните следующие действия:

   a. Если требуется, укажите другую папку, в которой будут сохранены устанавливаемые файлы.

   b. Нажмите на кнопку **Далее**.

9. В окне **Готовность к установке** нажмите на кнопку **Установить**.

   Мастер приступит к установке выбранных компонентов.

10. Нажмите на кнопку **Готово**.

    Работа мастера установки будет завершена. Консоль программы будет установлена на защищаемом устройстве.

Если вы установили набор Средства администрирования не на защищаемом устройстве, а на другом устройстве сети, выполните дополнительную настройку.

Дополнительная настройка после установки Консоли программы на другое устройство

Если вы установили Консоль программы не на защищаемом устройстве, а на другом устройстве сети, выполните следующие действия для того, чтобы пользователи могли удаленно управлять Kaspersky Embedded Systems Security:

- На защищаемом устройстве добавьте пользователей Kaspersky Embedded Systems Security в группу ESS Administrators.

- Включите сетевые соединения для службы Kaspersky Security Management Service (kavfsgt.exe), если на защищаемом сервере используется брандмауэр Windows или сетевой экран стороннего поставщика.

- Если во время установки Консоли программы на устройство под управлением Microsoft Windows не был установлен флажок **Разрешить удаленный доступ**, вручную включите сетевые соединения для Консоли программы через сетевой экран устройства.

Консоль программы на удаленном устройстве использует протокол DCOM для получения информации о событиях Kaspersky Embedded Systems Security, например, о проверенных объектах или о завершении задач, от службы Kaspersky Security Management на защищаемом устройстве. Необходимо разрешить сетевые соединения для Консоли программы в параметрах брандмауэра Windows, чтобы устанавливать соединения между Консолью программы и службой Kaspersky Security Management.

На удаленном устройстве, на котором установлена Консоль программы, выполните следующие действия:

- Убедитесь, что разрешен анонимный удаленный доступ к программам COM (но не удаленный запуск и активация программ COM).
- В параметрах брандмауэра Windows откройте порт TCP 135 и разрешите сетевые соединения для исполняемого файла процесса удаленного управления Kaspersky Embedded Systems Security – kavfsrcn.exe.

  Устройство, на котором установлена Консоль программы, обменивается информацией с защищаемым устройством через порт TCP 135.
- Чтобы разрешить подключение, настройте правило исходящего подключения для брандмауэра Windows.

  В отличие от стандартных служб TCP/IP и UDP/IP, где для каждого протокола имеется фиксированный порт, DCOM динамически назначает порты удаленным COM-объектам. Если между клиентским устройством (на котором установлена Консоль программы) и DCOM-устройством (защищаемым устройством) находится сетевой экран, нужно открыть широкий диапазон портов.

Аналогичные шаги следует выполнить для настройки любого другого программного или аппаратного сетевого экрана.

Если Консоль программы открыта во время настройки соединения между защищаемым устройством и устройством, на котором установлена Консоль программы, выполните следующие действия:

1. Закройте Консоль программы.
2. Дождитесь завершения процесса удаленного управления Kaspersky Embedded Systems Security – kavfsrcn.exe.
3. Перезапустите Консоль программы.

   Будут применены новые параметры соединения.

Разрешение анонимного удаленного доступа к программам COM

Названия параметров могут отличаться в разных операционных системах Windows.

Чтобы разрешить анонимный удаленный доступ к программам COM, выполните следующие действия:

1. На удаленном устройстве, на котором установлена Консоль Kaspersky Embedded Systems Security, откройте консоль Службы компонентов.
2. Выберите **Пуск** → **Выполнить**.
3. Введите команду `dcomcnfg`.

4. Нажмите на кнопку **OK**.
5. В консоли **Службы компонентов** защищаемого устройства разверните узел **Компьютеры**.
6. Откройте контекстное меню узла **Мой компьютер**.
7. Выберите пункт **Свойства**.
8. В окне **Свойства** на закладке **Безопасность COM** нажмите на кнопку **Изменить ограничения** в блоке параметров **Права доступа**.
9. В окне **Разрешение на доступ** убедитесь, что для пользователя ANONYMOUS LOGON установлен флажок **Разрешить удаленный доступ**.
10. Нажмите на кнопку **OK**.

Разрешение сетевых соединений для процесса удаленного управления Kaspersky Embedded Systems Security

Названия параметров могут отличаться в разных операционных системах Windows.

Чтобы открыть TCP-порт 135 в брандмауэре Windows и разрешить сетевые соединения для процесса удаленного управления Kaspersky Embedded Systems Security, выполните следующие действия:

1. На удаленном устройстве закройте Консоль Kaspersky Embedded Systems Security.
2. Выполните одно из следующих действий:
   - В Microsoft Windows XP с пакетом обновлений 2 и выше:
     a. Выберите **Пуск** > **Брандмауэр Windows**.
     b. В окне **Брандмауэр Windows** (или Параметры брандмауэра Windows) на закладке **Исключения** нажмите на кнопку **Добавить порт**.
     c. В поле **Имя** укажите имя порта RPC (TCP/135) или задайте другое имя, например, DCOM Kaspersky Embedded Systems Security, а в поле **Номер порта** укажите номер порта: 135.
     d. Выберите протокол **TCP**.
     e. Нажмите на кнопку **OK**.
     f. На закладке **Исключения** нажмите на кнопку **Добавить программу**.
   - В Microsoft Windows 7 и выше:
     a. Выберите **Пуск** > **Панель управления** > **Брандмауэр Windows**.
     b. В окне **Брандмауэр Windows** выберите пункт **Разрешить запуск программы или компонента через брандмауэр Windows**.

c. В окне **Разрешить связь программ через брандмауэр Windows** нажмите на кнопку **Разрешить другую программу**.

3. В окне **Добавление программы** укажите файл kavfsrcn.exe. Он хранится в папке, которую вы указали в качестве папки назначения при установке Консоли Kaspersky Embedded Systems Security с помощью Microsoft Management Console.

4. Нажмите на кнопку **OK**.

5. Нажмите на кнопку **OK** в окне **Брандмауэр Windows (Параметры брандмауэра Windows)**.

Добавление правила исходящего подключения для брандмауэра Windows

Названия параметров могут отличаться в разных операционных системах Windows.

Чтобы добавить правило исходящего подключения для брандмауэра Windows, выполните следующие действия:

1. Выберите **Пуск** > **Панель управления** > **Брандмауэр Windows**.

2. В окне **Брандмауэр Windows** перейдите по ссылке **Дополнительные параметры**.

   Откроется окно **Брандмауэр Windows в режиме повышенной безопасности**.

3. Выберите вложенный узел **Правила для исходящего подключения**.

4. На панели **Действия** выберите пункт **Создать правило**.

5. В открывшемся окне **Мастер создания правила для нового исходящего подключения** выберите параметр **Порт** и нажмите на кнопку **Далее**.

6. Выберите протокол **TCP**.

7. В поле **Определенные удаленные порты** укажите следующий диапазон портов, чтобы разрешить исходящие подключения: 1024–65535.

8. В окне **Действие** выберите пункт **Разрешить подключение**.

9. Сохраните созданное правило и закройте окно **Брандмауэр Windows в режиме повышенной безопасности**.

Брандмауэр Windows не разрешает установку сетевых соединений между Консолью программы и службой Kaspersky Security Management.

Действия после установки Kaspersky Embedded Systems Security

Kaspersky Embedded Systems Security запускает задачи защиты и проверки сразу после установки, если вы активировали программу. Если во время установки Kaspersky Embedded Systems Security был установлен флажок **Включить постоянную защиту после установки программы** (по умолчанию), программа проверяет объекты файловой системы устройства при доступе к ним. Каждую пятницу в 20:00 Kaspersky Embedded Systems Security выполняет задачу Проверка важных областей.

После установки Kaspersky Embedded Systems Security рекомендуется выполнить следующие действия:

- Запустить задачу обновления баз программы. После установки Kaspersky Embedded Systems Security проверяет объекты с использованием баз, которые входили в состав программы при поставке.

  Рекомендуется сразу же обновить базы Kaspersky Embedded Systems Security, так как базы могли устареть.

  Далее программа будет обновлять базы каждый час согласно расписанию, установленному в задаче по умолчанию.

- Выполнить Проверку важных областей, если перед установкой Kaspersky Embedded Systems Security на устройстве не была установлена антивирусная программа с включенной функцией постоянной защиты файлов.

- Настроить уведомления администратора о событиях Kaspersky Embedded Systems Security.

Запуск и настройка задачи Обновление баз программы

Чтобы обновить базы программы после установки, выполните следующие действия:

1. В свойствах задачи обновления баз программы настройте соединение с источником обновлений – HTTP- или FTP-серверами обновлений "Лаборатории Касперского".

2. Запустите задачу Обновление баз программы.

В вашей сети может быть не настроен протокол Web Proxy Auto-Discovery Protocol (WPAD) для автоматического распознавания параметров прокси-сервера в локальной сети. В этом случае может потребоваться проверка подлинности при доступе к прокси-серверу.

Чтобы указать дополнительные параметры прокси-сервера и параметры проверки подлинности для доступа к прокси-серверу, выполните следующие действия:

1. Откройте контекстное меню узла **Kaspersky Embedded Systems Security**.

2. Выберите пункт **Свойства**.

   Откроется окно **Параметры программы**.

3. Выберите закладку **Параметры соединения**.

4. В разделе **Параметры прокси-сервера** установите флажок **Использовать параметры указанного прокси-сервера**.

5. В поле **Адрес** укажите адрес прокси-сервера, а в поле **Порт** укажите номер порта прокси-сервера.

6. В разделе **Параметры аутентификации на прокси-сервере** выберите требуемый метод аутентификации из раскрывающегося списка:

   - **Использовать NTLM-аутентификацию**, если прокси-сервер поддерживает встроенную в Windows проверку подлинности NTLM. Kaspersky Embedded Systems Security будет использовать для доступа к

прокси-серверу учетную запись, указанную в параметрах задачи. По умолчанию задача запускается под учетной записью **Локальная система** (**SYSTEM**).

- **Использовать NTLM-аутентификацию с именем пользователя и паролем**, если прокси-сервер поддерживает встроенную в Windows проверку подлинности NTLM. Kaspersky Embedded Systems Security будет использовать указанную учетную запись для доступа к прокси-серверу. Введите имя и пароль пользователя или выберите пользователя в списке.

- **Использовать имя пользователя и пароль**, чтобы выбрать обычную проверку подлинности. Введите имя и пароль пользователя или выберите пользователя в списке.

7. В окне **Параметры программы** нажмите на кнопку **OK**.

Чтобы настроить соединение с серверами обновлений "Лаборатории Касперского" в задаче обновления баз программы, выполните следующие действия:

1. Запустите Консоль программы одним из следующих способов:

   - Откройте Консоль программы на защищаемом устройстве. Для этого в меню **Пуск** выберите **Все программы** > **Kaspersky Embedded Systems Security** > **Средства администрирования** > **Консоль Kaspersky Embedded Systems Security**.

   - Если Консоль программы запущена не на защищаемом устройстве, подключитесь к защищаемому устройству:

     a. В дереве Консоли программы откройте контекстное меню узла **Kaspersky Embedded Systems Security**.

     b. Выберите пункт **Подключиться к другому компьютеру**.

     c. В окне **Выбор сервера** выберите **Другой сервер** и в поле ввода укажите сетевое имя защищаемого устройства.

     Если учетная запись, которую вы использовали для входа в Microsoft Windows, не обладает правами доступа к службе Kaspersky Security Management, укажите учетную запись, которая обладает этими правами.

   Откроется окно Консоли программы.

2. В дереве Консоли программы разверните узел **Обновление**.

3. Выберите вложенный узел **Обновление баз программы**.

4. В панели результатов перейдите по ссылке **Свойства**.

5. В открывшемся окне **Параметры задачи** выберите закладку **Параметры соединения**.

6. Выберите **Использовать параметры прокси-сервера для соединения с серверами обновлений "Лаборатории Касперского"**.

7. В окне **Параметры задачи** нажмите на кнопку **OK**.

Параметры соединения с источником обновлений в задаче Обновление баз программы будут сохранены.

Чтобы запустить задачу Обновление баз программы, выполните следующие действия:

1. В дереве Консоли программы разверните узел **Обновление**.
2. В контекстном меню вложенного узла **Обновление баз программы** выберите пункт **Запустить**.

   Задача Обновление баз программы будет запущена.

   После успешного завершения задачи можно посмотреть дату выпуска последних установленных обновлений баз программы в панели результатов узла **Kaspersky Embedded Systems Security**.

Проверка важных областей

После того как вы обновили базы Kaspersky Embedded Systems Security, проверьте защищаемое устройство на наличие вредоносных программ с помощью задачи Проверка важных областей.

Чтобы запустить задачу Проверка важных областей, выполните следующие действия:

1. В дереве Консоли программы разверните узел **Проверка по требованию**.
2. В контекстном меню вложенного узла **Проверка важных областей** выберите команду **Запустить**.

Задача будет запущена; в панели результатов отобразится статус задачи **Выполняется**.

Чтобы просмотреть журнал выполнения задачи,

в панели результатов узла **Проверка важных областей** перейдите по ссылке **Открыть журнал выполнения**.

Изменение состава компонентов и восстановление Kaspersky Embedded Systems Security

Вы можете добавлять или удалять компоненты Kaspersky Embedded Systems Security. Вам нужно предварительно остановить задачу Постоянная защита файлов, если вы хотите удалить компонент Постоянная защита файлов. В остальных случаях останавливать задачу Постоянная защита файлов или службу Kaspersky Security не требуется.

Если доступ к управлению программой защищен паролем, Kaspersky Embedded Systems Security запрашивает ввод пароля при попытке удаления или изменения состава программных компонентов в мастере установки.

Чтобы изменить состав компонентов Kaspersky Embedded Systems Security, выполните следующие действия:

1. В меню **Пуск** выберите **Все программы** > **Kaspersky Embedded Systems Security** > **Изменение или удаление Kaspersky Embedded Systems Security**.

   Откроется окно мастера установки программы **Изменение, восстановление или удаление**.

2. Выберите **Изменение состава компонентов программы**. Нажмите на кнопку **Далее**.

   Откроется окно **Выборочная установка**.

3. В списке доступных компонентов в окне **Выборочная установка** выберите компоненты, которые требуется добавить или удалить из состава Kaspersky Embedded Systems Security. Для этого выполните следующие действия:

- Чтобы изменить состав компонентов, нажмите на кнопку рядом с названием выбранного компонента. В контекстном меню выберите:

  - пункт **Компонент будет установлен на локальный жесткий диск**, если требуется установить отдельный компонент;

  - пункт **Компонент и его подкомпоненты будут установлены на локальный жесткий диск**, если требуется установить группу компонентов.

- Чтобы удалить установленные ранее компоненты, нажмите на кнопку рядом с названием выбранного компонента. В контекстном меню выберите пункт **Компонент будет недоступен**.

Нажмите на кнопку **Далее**.

4. В окне **Готовность к установке** подтвердите изменение состава компонентов программы, нажав на кнопку **Установить**.

5. В окне, открывшемся по завершении установки, нажмите на кнопку **ОК**.

Состав компонентов Kaspersky Embedded Systems Security будет изменен в соответствии с заданными параметрами.

Если в работе Kaspersky Embedded Systems Security возникли проблемы (Kaspersky Embedded Systems Security завершается аварийно, задачи завершаются аварийно или не запускаются), можно попробовать восстановить Kaspersky Embedded Systems Security. Вы можете выполнить восстановление с сохранением текущих значений параметров Kaspersky Embedded Systems Security или выбрать режим, при котором все параметры Kaspersky Embedded Systems Security примут значения по умолчанию.

Чтобы восстановить Kaspersky Embedded Systems Security после аварийного завершения работы программы или задач, выполните следующие действия:

1. В меню **Пуск** выберите пункт **Все программы**.

2. Выберите **Kaspersky Embedded Systems Security**.

3. Выберите **Изменение или удаление Kaspersky Embedded Systems Security**.

   Откроется окно мастера установки программы **Изменение, восстановление или удаление**.

4. Выберите вариант **Восстановление установленных компонентов**. Нажмите на кнопку **Далее**.

   Откроется окно **Восстановление установленных компонентов**.

5. В окне **Восстановление установленных компонентов** установите флажок **Восстановить рекомендуемые параметры работы программы**, если вы хотите сбросить параметры программы и восстановить Kaspersky Embedded Systems Security с параметрами по умолчанию. Нажмите на кнопку **Далее**.

6. В окне **Готовность к восстановлению** подтвердите операцию восстановления программы, нажав на кнопку **Установить**.

7. В окне, открывшемся по завершении операции восстановления, нажмите на кнопку **ОК**.

Программа Kaspersky Embedded Systems Security будет восстановлена с указанными параметрами.

Удаление с помощью мастера установки

В этом разделе приведены инструкции по удалению Kaspersky Embedded Systems Security и Консоли программы с защищаемого устройства с помощью мастера установки / удаления.

Удаление Kaspersky Embedded Systems Security

Файлы дампа и трассировки не удаляются при удалении Kaspersky Embedded Systems Security. Можно вручную удалить файлы дампа и трассировки из папки, указанной при настройке записи файлов дампа и трассировки.

Названия параметров могут отличаться в разных операционных системах Windows.

Вы можете удалить Kaspersky Embedded Systems Security с защищаемого устройства с помощью мастера установки / удаления.

После удаления Kaspersky Embedded Systems Security с защищаемого устройства может потребоваться перезагрузка. Перезагрузку можно отложить.

Удаление, восстановление и установка программы через панель управления Windows невозможна, если операционная система использует функцию Контроль учетных записей (User Account Control) или если доступ к управлению программой защищен паролем.

Если доступ к управлению программой защищен паролем, Kaspersky Embedded Systems Security запрашивает ввод пароля при попытке удаления или изменения состава программных компонентов в мастере установки.

Чтобы удалить Kaspersky Embedded Systems Security, выполните следующие действия:

1. В меню **Пуск** выберите пункт **Все программы**.
2. Выберите **Kaspersky Embedded Systems Security**.
3. Выберите **Изменение или удаление Kaspersky Embedded Systems Security**.

   Откроется окно мастера установки программы **Изменение, восстановление или удаление**.
4. Выберите пункт **Удаление компонентов программы**. Нажмите на кнопку **Далее**.

   Откроется окно **Дополнительные параметры удаления программы**.
5. Если требуется, в окне **Дополнительные параметры удаления программы** выполните следующие действия:

   a. Установите флажок **Экспортировать объекты на карантине**, чтобы программа Kaspersky Embedded Systems Security экспортировала объекты, помещенные на карантин. По умолчанию флажок снят.

   b. Установите флажок **Экспортировать объекты резервного хранилища**, чтобы экспортировать объекты из резервного хранилища Kaspersky Embedded Systems Security. По умолчанию флажок снят.

c. Нажмите на кнопку **Сохранить в** и укажите папку, в которую требуется экспортировать объекты. По умолчанию экспорт объектов осуществляется в папку %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\Uninstall.

   Нажмите на кнопку **Далее**.

6. В окне **Готовность к удалению** подтвердите удаление, нажав на кнопку **Удалить**.

7. В окне, открывшемся по завершении удаления, нажмите на кнопку **OK**.

Программа Kaspersky Embedded Systems Security будет удалена с защищаемого устройства.

Удаление Консоли Kaspersky Embedded Systems Security

Названия параметров могут отличаться в разных операционных системах Windows.

Вы можете удалить Консоль программы с защищаемого устройства с помощью мастера установки / удаления.

После удаления Консоли программы перезагрузка защищаемого устройства не требуется.

Чтобы удалить Консоль программы, выполните следующие действия:

1. В меню **Пуск** выберите пункт **Все программы**.

2. Выберите **Kaspersky Embedded Systems Security**.

3. Выберите **Изменение или удаление Средств администрирования Kaspersky Embedded Systems Security**.

   Откроется окно мастера **Изменение, восстановление или удаление**.

4. Выберите пункт **Удаление компонентов программы** и нажмите на кнопку **Далее**.

5. Откроется окно **Готовность к удалению**. Нажмите на кнопку **Удалить**.

   Откроется окно **Удаление завершено**.

6. Нажмите на кнопку **OK**.

Операция удаления будет завершена; окно мастера установки будет закрыто.

Установка и удаление программы из командной строки

Этот раздел содержит описание особенностей установки и удаления Kaspersky Embedded Systems Security из командной строки, примеры команд для установки и удаления Kaspersky Embedded Systems Security из командной строки, примеры команд для добавления и удаления компонентов Kaspersky Embedded Systems Security из командной строки.

Об установке и удалении Kaspersky Embedded Systems Security из командной строки

Файлы дампа и трассировки не удаляются при удалении Kaspersky Embedded Systems Security. Можно вручную удалить файлы дампа и трассировки из папки, указанной при настройке записи файлов дампа и трассировки.

Вы можете устанавливать и удалять Kaspersky Embedded Systems Security, добавлять или удалять его компоненты, запустив из командной строки файлы пакета установки \product\ess_x86.msi или \product\ess_x64.msi и указав параметры установки с помощью ключей.

Вы можете установить набор "Средства администрирования" на защищаемом устройстве или на другом устройстве в сети, чтобы работать с Консолью программы локально или удаленно. Для этого используйте пакет установки \console\esstools.msi.

Выполняйте установку с правами учетной записи, входящей в группу администраторов на защищаемом устройстве, на котором установлена программа.

Если вы запустите на защищаемом устройстве один из файлов \product\ess_x86.msi или \product\ess_x64.msi без дополнительных ключей, программа Kaspersky Embedded Systems Security будет установлена с рекомендуемыми параметрами установки.

Вы можете задать набор устанавливаемых компонентов с помощью ключа ADDLOCAL, перечислив в качестве его значений коды выбранных компонентов или наборов компонентов.

Примеры команд установки Kaspersky Embedded Systems Security

В этом разделе приведены примеры команд для установки Kaspersky Embedded Systems Security.

На защищаемом устройстве под управлением 32-разрядной версии Microsoft Windows запускайте файлы с суффиксом x86 из комплекта поставки. На защищаемом устройстве под управлением 64-разрядной версии Microsoft Windows запускайте файлы с суффиксом x64 из комплекта поставки.

Подробная информация об использовании стандартных команд и ключей установщика Windows содержится в документации, предоставляемой корпорацией Microsoft.

Примеры установки Kaspersky Embedded Systems Security из файла setup.exe

Чтобы установить Kaspersky Embedded Systems Security с параметрами по умолчанию без взаимодействия с пользователем, выполните следующую команду:

```
\product\setup.exe /s/p EULA=1 PRIVACYPOLICY=1
```

Можно установить Kaspersky Embedded Systems Security со следующими параметрами:

- установить только компоненты Постоянная защита файлов и Проверка по требованию;

- не запускать Постоянную защиту файлов при запуске Kaspersky Embedded Systems Security;
- не исключать из проверки файлы, рекомендованные к исключению корпорацией Microsoft.

Для этого выполните следующую команду:

```
\product\setup.exe /p "ADDLOCAL=Oas RUNRTP=0 ADDMSEXCLUSION=0"
```

Примеры команд для установки: запуск msi-файла

Чтобы установить Kaspersky Embedded Systems Security с параметрами по умолчанию без взаимодействия с пользователем, выполните следующую команду:

```
msiexec /i ess.msi /qn EULA=1 PRIVACYPOLICY=1
```

Чтобы установить Kaspersky Embedded Systems Security с параметрами по умолчанию и показать интерфейс установки, выполните следующую команду:

```
msiexec /i ess.msi /qf EULA=1 PRIVACYPOLICY=1
```

Чтобы установить Kaspersky Embedded Systems Security и активировать его с помощью файла ключа C:\0000000A.key, выполните следующую команду:

```
msiexec /i ess.msi LICENSEKEYPATH=C:\0000000A.key /qn EULA=1 PRIVACYPOLICY=1
```

Чтобы установить Kaspersky Embedded Systems Security с предварительной проверкой активных процессов и загрузочных секторов локальных дисков, выполните следующую команду:

```
msiexec /i ess.msi PRESCAN=1 /qn EULA=1 PRIVACYPOLICY=1
```

Чтобы установить Kaspersky Embedded Systems Security в папку установки C:\ESS, выполните следующую команду:

```
msiexec /i ess.msi INSTALLDIR=C:\ESS /qn EULA=1 PRIVACYPOLICY=1
```

Чтобы установить Kaspersky Embedded Systems Security и сохранить файл журнала установки с именем ess.log в папку, где хранится msi-файл Kaspersky Embedded Systems Security, выполните следующую команду:

```
msiexec /i ess.msi /l*v ess.log /qn EULA=1 PRIVACYPOLICY=1
```

Чтобы установить Консоль Kaspersky Embedded Systems Security, выполните следующую команду:

```
msiexec /i esstools.msi /qn EULA=1
```

Чтобы установить Kaspersky Embedded Systems Security и активировать программу с помощью файла ключа C:\0000000A.key, а также настроить Kaspersky Embedded Systems Security в соответствии с параметрами в конфигурационном файле C:\settings.xml, выполните следующую команду:

```
msiexec /i ess.msi LICENSEKEYPATH=C:\0000000A.key CONFIGPATH=C:\settings.xml /qn EULA=1
PRIVACYPOLICY=1
```

Чтобы установить исправление, если программа Kaspersky Embedded Systems Security защищена паролем, выполните следующую команду:

```
msiexec /p "<msp путь к имени файла>" UNLOCK_PASSWORD=<пароль>
```

Действия после установки Kaspersky Embedded Systems Security

Kaspersky Embedded Systems Security запускает задачи защиты и проверки сразу после установки, если вы активировали программу. Если во время установки Kaspersky Embedded Systems Security был установлен флажок **Включить постоянную защиту после установки программы**, программа проверяет объекты файловой системы устройства при доступе к ним. Каждую пятницу в 20:00 Kaspersky Embedded Systems Security выполняет задачу Проверка важных областей.

После установки Kaspersky Embedded Systems Security рекомендуется выполнить следующие действия:

- Запустить задачу обновления баз Kaspersky Embedded Systems Security. После установки Kaspersky Embedded Systems Security проверяет объекты с использованием баз, которые входили в состав программы при поставке. Рекомендуется сразу же обновить базы Kaspersky Embedded Systems Security. Для этого вам нужно запустить задачу Обновление баз программы. Далее обновление баз будет выполняться каждый час согласно расписанию, установленному по умолчанию.

  Например, вы можете запустить задачу Обновление баз программы, выполнив следующую команду:

  KAVSHELL UPDATE /KL /PROXY:proxy.company.com:8080 /AUTHTYPE:1 /PROXYUSER:inetuser /PROXYPWD:123456

  При этом обновления баз Kaspersky Embedded Systems Security будут загружены с серверов обновлений "Лаборатории Касперского". Соединение с источником обновлений происходит через прокси-сервер (адрес прокси-сервера: proxy.company.com, порт: 8080) с использованием для доступа к серверу встроенной в Windows проверки подлинности NTLM с учетной записью (имя пользователя: inetuser; пароль: 123456).

- Выполнить Проверку важных областей, если перед установкой Kaspersky Embedded Systems Security на устройстве не была установлена антивирусная программа с включенной функцией постоянной защиты файлов.

Чтобы выполнить задачу Проверка важных областей с помощью командной строки, выполните следующую команду:

KAVSHELL SCANCRITICAL /W:scancritical.log

Эта команда сохраняет журнал выполнения задачи в файле scancritical.log в текущей папке.

- Настроить уведомления администратора о событиях Kaspersky Embedded Systems Security.

Добавление и удаление компонентов. Примеры команд

Компонент Проверка по требованию устанавливается автоматически. Вам не нужно указывать его в списке значений ключа ADDLOCAL, добавляя или удаляя компоненты Kaspersky Embedded Systems Security.

Чтобы добавить компонент Контроль запуска программ к ранее установленным компонентам, выполните следующую команду:

```
msiexec /i ess.msi ADDLOCAL=Oas,AppCtrl /qn
```

или

```
\product\setup.exe /s /p "ADDLOCAL=Oas,AppCtrl"
```

Если вы перечислите не только компоненты, которые требуется установить, но и уже установленные компоненты, Kaspersky Embedded Systems Security переустановит указанные установленные компоненты.

Чтобы удалить установленные компоненты, выполните следующую команду:

```
msiexec /i ess.msi
"ADDLOCAL=Oas,Ods,Ksn,AntiExploit,DevCtrl,Firewall,AntiCryptor,LogInspector,AKIntegratio
REMOVE=AppCtrl,Fim" /qn
```

Удаление Kaspersky Embedded Systems Security. Примеры команд

Чтобы удалить Kaspersky Embedded Systems Security с защищаемого устройства, выполните следующую команду:

```
msiexec /x ess.msi /qn
```

или

- Для 32-разрядной операционной системы:
  `msiexec /x {51AACF7F-421E-40FA-B2B7-FCFE0BACF505} /qn`
- Для 64-разрядной операционной системы:
  `msiexec /x {673F3697-9D6C-4CF4-BB28-478492F45DDC} /qn`

Чтобы удалить Консоль Kaspersky Embedded Systems Security, выполните следующую команду:

```
msiexec /x esstools.msi /qn
```

или

- Для 32-разрядной операционной системы:
  `msiexec /x {26E7C356-E535-4434-9AB1-F1EA4E8A70F4} /qn`
- Для 64-разрядной операционной системы:
  `msiexec /x {7EC1A40D-52F4-4F8F-93BA-F6E68B152C26} /qn`

Чтобы удалить Kaspersky Embedded Systems Security с устройства, на котором установлена защита паролем, выполните следующую команду:

- Для 32-разрядной операционной системы:
  `msiexec /x {51AACF7F-421E-40FA-B2B7-FCFE0BACF505} UNLOCK_PASSWORD=*** /qn`
- Для 64-разрядной операционной системы:
  `msiexec /x {673F3697-9D6C-4CF4-BB28-478492F45DDC} UNLOCK_PASSWORD=*** /qn`

Коды возврата

В таблице ниже приведено описание кодов возврата командной строки.

Коды возврата

Код	Описание

1324	Имя папки назначения содержит недопустимые символы.
25001	Недостаточно прав для установки Kaspersky Embedded Systems Security. Чтобы установить программу, запустите мастер установки с правами локального администратора.
25003	Не удается установить Kaspersky Embedded Systems Security на устройство под управлением этой версии Microsoft Windows. Пожалуйста, запустите мастер установки программы, предназначенный для 64-разрядной версии Microsoft Windows.
25004	Обнаружено несовместимое программное обеспечение. Чтобы продолжить установку, удалите следующее программное обеспечение: <список несовместимого программного обеспечения>.
25010	Указанный путь не может быть использован для сохранения объектов на карантине.
25011	Имя папки для сохранения объектов на карантине содержит недопустимые символы.
26251	Не удалось загрузить DLL для Счетчиков производительности.
26252	Не удалось загрузить DLL для Счетчиков производительности.
27300	Драйвер не может быть установлен.
27301	Драйвер не может быть удален.
27302	Невозможно установить сетевой компонент. Достигнуто максимальное пороговое значение поддерживаемого количества устройств фильтрации.
27303	Антивирусные базы не найдены.

Установка и удаление программы с помощью Kaspersky Security Center

Этот раздел содержит информацию об установке Kaspersky Embedded Systems Security с помощью Kaspersky Security Center, описание процедуры установки и удаления Kaspersky Embedded Systems Security через Kaspersky Security Center, а также описание действий после установки Kaspersky Embedded Systems Security.

Общие сведения об установке через Kaspersky Security Center

Вы можете установить Kaspersky Embedded Systems Security через Kaspersky Security Center с помощью задачи удаленной установки.

После выполнения задачи удаленной установки программа Kaspersky Embedded Systems Security будет установлена с одинаковыми параметрами на несколько защищаемых устройств.

Можно объединить все защищаемые устройства в одну группу администрирования и создать групповую задачу установки Kaspersky Embedded Systems Security на защищаемые устройства этой группы.

Вы можете создать задачу удаленной установки Kaspersky Embedded Systems Security для набора защищаемых устройств, не объединенных в одну группу администрирования. При создании этой задачи нужно сформировать список отдельных защищаемых устройств, на которые требуется установить Kaspersky Embedded Systems Security.

Подробная информация о задаче удаленной установки приведена в *Справке Kaspersky Security Center*.

Права для установки или удаления Kaspersky Embedded Systems Security

Учетная запись, указанная в задаче удаленной установки (удаления), должна входить в группу администраторов на каждом защищаемом устройстве во всех случаях, кроме следующих ситуаций:

- На защищаемых устройствах, на которых требуется установить Kaspersky Embedded Systems Security, уже установлен Агент администрирования Kaspersky Security Center (независимо от того, в каком домене находятся защищаемые устройства и принадлежат ли они к какому-либо домену).

  Если Агент администрирования еще не установлен на защищаемых устройствах, вы можете установить его вместе с Kaspersky Embedded Systems Security с помощью задачи удаленной установки. Перед установкой Агента администрирования убедитесь, что учетная запись, которую вы укажете в задаче, входит в группу администраторов на каждом защищаемом устройстве.

- Все защищаемые устройства, на которые вы хотите установить Kaspersky Embedded Systems Security, находятся в одном домене с Сервером администрирования и Сервер администрирования зарегистрирован под учетной записью **Администратор домена** (Domain Admin), если эта учетная запись обладает правами локального администратора на защищаемых устройствах домена.

По умолчанию задача удаленной установки методом **Форсированная установка** запускается с правами той учетной записи, под которой работает Сервер администрирования.

В групповых задачах и в задачах для набора защищаемых устройств, в которых был выбран метод форсированной установки (удаления), учетная запись должна обладать следующими правами на защищаемом устройстве:

- правом на удаленный запуск программ;
- доступом к папке общего доступа **Admin$**;
- правом **Вход в качестве службы**.

Установка Kaspersky Embedded Systems Security с помощью Kaspersky Security Center

Подробная информация о формировании инсталляционного пакета о и создании задачи удаленной установки содержится в Руководстве по внедрению Kaspersky Security Center.

Если вы планируете в дальнейшем управлять Kaspersky Embedded Systems Security через Kaspersky Security Center, убедитесь, что выполняются следующие условия:

- На защищаемом устройстве с установленным Сервером администрирования Kaspersky Security Center также установлен Плагин управления (файл \product\klcfginst.exe комплекта поставки Kaspersky Embedded Systems Security).
- На защищаемых устройствах установлен Агент администрирования Kaspersky Security Center. Если на защищаемых устройствах не установлен Агент администрирования Kaspersky Security Center, вы можете установить его вместе с Kaspersky Embedded Systems Security в задаче удаленной установки.

Можно также объединить устройства в группу администрирования, чтобы в дальнейшем управлять параметрами защиты с помощью политик и групповых задач Kaspersky Security Center.

Чтобы установить Kaspersky Embedded Systems Security с помощью задачи удаленной установки, выполните следующие действия:

1. Запустите Консоль администрирования Kaspersky Security Center.
2. В Kaspersky Security Center разверните узел **Дополнительно**.
3. Разверните вложенный узел **Удаленная установка**.
4. В рабочей области узла **Инсталляционные пакеты** нажмите на кнопку **Создать инсталляционный пакет**.
5. Выберите вариант **Создать инсталляционный пакет для программы "Лаборатории Касперского"**.
6. Введите имя инсталляционного пакета.
7. Выберите файл ess.kud из комплекта установки Kaspersky Embedded Systems Security в качестве файла инсталляционного пакета.

   Откроется окно **Лицензионное соглашение и Политика конфиденциальности**.
8. Если вы согласны с условиями и положениями Лицензионного соглашения и Политики конфиденциальности, для продолжения установки установите флажки **Я подтверждаю, что полностью прочитал, понимаю и принимаю положения и условия настоящего Лицензионного соглашения** и **Я понимаю и соглашаюсь, что мои данные будут обрабатываться и пересылаться (в том числе в третьи страны), согласно «Политике конфиденциальности». Я подтверждаю, что полностью прочитал и понимаю «Политику конфиденциальности»**.

   Вам нужно принять условия Лицензионного соглашения и Политики конфиденциальности для продолжения установки.
9. Чтобы изменить набор устанавливаемых компонентов Kaspersky Embedded Systems Security и параметры установки по умолчанию в инсталляционном пакете, выполните следующие действия:

   a. В Kaspersky Security Center разверните узел **Удаленная установка**.

   b. В панели результатов вложенного узла **Инсталляционные пакеты** откройте контекстное меню созданного инсталляционного пакета Kaspersky Embedded Systems Security и выберите пункт **Свойства**.

   c. В окне **Свойства: <название инсталляционного пакета>** перейдите раздел **Настройка**.

      В группе параметров **Устанавливаемые компоненты** установите флажки рядом с названиями компонентов Kaspersky Embedded Systems Security, которые вы хотите установить.

   d. Чтобы указать папку назначения, отличную от папки, установленной по умолчанию, укажите имя папки и путь к ней в поле **Папка назначения**.

      Путь к папке назначения может содержать системные переменные окружения. Если указанной папки не существует на защищаемом устройстве, она будет создана.

   e. В группе параметров **Дополнительные параметры установки** настройте следующие параметры:

      - **Выполнить антивирусную проверку защищаемого устройства перед началом установки**
      - **Включить постоянную защиту после установки программы**

- **Добавить к исключениям файлы, рекомендованные Microsoft**
- **Добавить к исключениям файлы, рекомендованные Лабораторией Касперского**

f. В диалоговом окне **Свойства: <название инсталляционного пакета>** нажмите на кнопку **ОК**.

10. В узле **Инсталляционные пакеты** создайте задачу удаленной установки Kaspersky Embedded Systems Security на защищаемые устройства (группу администрирования). Настройте параметры задачи.

    Подробная информация о создании и настройке задачи удаленной установки приведена в *Справке Kaspersky Security Center*.

11. Запустите задачу удаленной установки Kaspersky Embedded Systems Security.

Программа Kaspersky Embedded Systems Security будет установлена на указанные в задаче защищаемые устройства.

Действия после установки Kaspersky Embedded Systems Security

После установки Kaspersky Embedded Systems Security рекомендуется обновить базы Kaspersky Embedded Systems Security на устройствах, а также выполнить Проверку важных областей устройств, если до установки Kaspersky Embedded Systems Security на устройствах не были установлены антивирусные программы с включенной функцией постоянной защиты.

Если защищаемые устройства, на которых установлена программа Kaspersky Embedded Systems Security, объединены в одну группу администрирования в Kaspersky Security Center, можно выполнить эти задачи следующими способами:

1. Создать задачу обновления баз программы для группы защищаемых устройств, на которых установлена программа Kaspersky Embedded Systems Security. Установить Сервер администрирования Kaspersky Security Center в качестве источника обновлений.

2. Создать групповую задачу проверки по требованию со статусом Проверка важных областей. Kaspersky Security Center оценивает состояние безопасности каждого защищаемого устройства группы по результатам выполнения этой задачи, а не по результатам задачи Проверка важных областей.

3. Создать новую политику для группы защищаемых устройств. В свойствах политики в разделе **Параметры программы** выключить запуск по расписанию системных задач проверки по требованию и задачи Обновление баз программы на защищаемых устройствах группы администрирования в подразделе **Запуск системных задач**.

Можно также настроить уведомления администратора о событиях Kaspersky Embedded Systems Security.

Установка Консоли программы через Kaspersky Security Center

Подробная информация о создании инсталляционного пакета и задачи удаленной установки содержится в Руководстве по внедрению Kaspersky Security Center.

Чтобы установить Консоль программы с помощью задачи удаленной установки, выполните следующие действия:

1. В Консоли администрирования Kaspersky Security Center разверните узел **Дополнительно**.

2. Разверните вложенный узел **Удаленная установка**.

3. В рабочей области узла Инсталляционные пакеты нажмите на кнопку **Создать инсталляционный пакет**. При создании нового инсталляционного пакета:

   a. В окне **Мастер создания инсталляционного пакета** выберите пункт **Создать инсталляционный пакет для указанного исполняемого файла** в качестве типа пакета.

   b. Введите имя инсталляционного пакета.

   c. В папке комплекта поставки Kaspersky Embedded Systems Security выберите файл \console\setup.exe и установите флажок **Копировать всю папку в инсталляционный пакет**.

   d. Если требуется, с помощью ключа командной строки ADDLOCAL измените состав устанавливаемых компонентов в поле **Параметры запуска исполняемого файла (необязательно)** и папку назначения.

   Например, чтобы установить только Консоль программы в папку C:\KasperskyConsole, не устанавливая файлы справки и документации, используйте следующие ключи командной строки:

   ```
   /s /p "ADDLOCAL=MmcSnapin INSTALLDIR=C:\KasperskyConsole EULA=1"
   ```

4. В узле **Инсталляционные пакеты** создайте задачу удаленной установки Консоли программы на выбранные защищаемые устройства (группу администрирования). Настройте параметры задачи.

   Подробная информация о создании и настройке задач удаленной установки приведена в Справке Kaspersky Security Center.

5. Запустите задачу удаленной установки.

Консоль программы будет установлена на указанные в задаче защищаемые устройства.

Удаление Kaspersky Embedded Systems Security с помощью Kaspersky Security Center

Файлы дампа и трассировки не удаляются при удалении Kaspersky Embedded Systems Security. Можно вручную удалить файлы дампа и трассировки из папки, указанной при настройке записи файлов дампа и трассировки.

Если доступ к управлению Kaspersky Embedded Systems Security на устройствах сети защищен паролем, введите пароль при создании задачи удаления нескольких программ. Если защита паролем не управляется политикой Kaspersky Security Center централизованно, программа Kaspersky Embedded Systems Security будет успешно удалена с устройств, где доступ к управлению программой защищен паролем, совпавшим с введенным значением. Программа Kaspersky Embedded Systems Security не будет удалена с других защищаемых устройств.

Чтобы удалить Kaspersky Embedded Systems Security, выполните следующие действия:

1. В Консоли администрирования Kaspersky Security Center создайте и запустите задачу удаления программы.

2. В задаче выберите метод удаления (аналогично выбору метода установки, см. предыдущий раздел) и укажите учетную запись, с правами которой Сервер администрирования будет обращаться к

защищаемым устройствам. Kaspersky Embedded Systems Security можно удалить только с параметрами удаления по умолчанию.

Установка и удаление программы через групповые политики Active Directory

Этот раздел содержит описание установки и удаления Kaspersky Embedded Systems Security через групповые политики Active Directory, а также информацию о действиях, которые требуется выполнить после установки Kaspersky Embedded Systems Security через групповые политики.

Установка Kaspersky Embedded Systems Security через групповые политики Active Directory

Вы можете установить Kaspersky Embedded Systems Security на несколько защищаемых устройств с помощью групповой политики Active Directory. Консоль программы можно установить аналогичным образом.

Защищаемые устройства, на которые требуется установить Kaspersky Embedded Systems Security или Консоль программы, должны быть в одном домене и в одной организационной единице.

Операционные системы защищаемых устройств, на которые требуется установить Kaspersky Embedded Systems Security с помощью политики, должны быть одной разрядности (32-разрядные или 64-разрядные).

Вы должны обладать правами администратора домена.

Чтобы установить Kaspersky Embedded Systems Security, используйте пакет установки ess_x86.msi или ess_x64.msi. Чтобы установить Консоль программы, используйте пакет установки esstools.msi.

> Подробная информация об использовании групповых политик Active Directory содержится в документации, предоставляемой корпорацией Microsoft.

Чтобы установить Kaspersky Embedded Systems Security (Консоль программы), выполните следующие действия:

1. Сохраните msi-файл, соответствующий разрядности установленной версии операционной системы Microsoft Windows, в папку общего доступа на контроллере домена.

2. Сохраните файл ключа в эту же общую папку на контроллере домена.

3. В этой же папке общего доступа на контроллере домена создайте файл install_props.json, содержащий приведенные ниже строки. Это означает, что вы соглашаетесь с условиями Лицензионного соглашения и Политики конфиденциальности.

   ```
   {
   "EULA": "1",
   "PRIVACYPOLICY": "1"
   }
   ```

4. На контроллере домена создайте новую политику для группы, в которую объединены защищаемые устройства.

5. С помощью **Редактора объектов групповых политик** создайте новый инсталляционный пакет в узле **Конфигурация компьютеров**. Укажите путь к msi-файлу Kaspersky Embedded Systems Security или Консоли программы в формате UNC (Universal Naming Convention).

6. Установите флажок установщика Windows **Всегда устанавливать с повышенными правами** как в узле **Конфигурация компьютеров**, так и в узле **Конфигурация пользователей** выбранной группы.

7. Примените изменения с помощью команды `gpupdate / force`.

Программа Kaspersky Embedded Systems Security будет установлена на защищаемые устройства группы после их перезагрузки.

Действия после установки Kaspersky Embedded Systems Security

После установки Kaspersky Embedded Systems Security на защищаемые устройства рекомендуется сразу обновить базы программы и выполнить Проверку важных областей. Эти действия можно выполнить из Консоли программы.

Можно также настроить уведомления администратора о событиях Kaspersky Embedded Systems Security.

Удаление Kaspersky Embedded Systems Security через групповые политики Active Directory

Файлы дампа и трассировки не удаляются при удалении Kaspersky Embedded Systems Security. Можно вручную удалить файлы дампа и трассировки из папки, указанной при настройке записи файлов дампа и трассировки.

Если вы установили Kaspersky Embedded Systems Security или Консоль программы в группе управляемых устройств, используя групповую политику Active Directory, вы можете использовать эту политику, чтобы удалить Kaspersky Embedded Systems Security или Консоль программы.

Вы можете удалить программу только с параметрами удаления по умолчанию.

Подробная информация об использовании групповых политик Active Directory содержится в документации, предоставляемой корпорацией Microsoft.

Если доступ к управлению программой защищен паролем, удаление Kaspersky Embedded Systems Security через групповые политики Active Directory невозможно.

Чтобы удалить Kaspersky Embedded Systems Security (или Консоль программы), выполните следующие действия:

1. На контроллере домена выберите организационную единицу, с защищаемых устройств которой требуется удалить Kaspersky Embedded Systems Security или Консоль программы.

2. Выберите политику, созданную для установки Kaspersky Embedded Systems Security, и в **Редакторе объектов групповых политик**, в узле **Установка программ** (**Конфигурация компьютеров** > **Параметры программ** > **Установка программ**) откройте контекстное меню пакета установки Kaspersky Embedded Systems Security (Консоли программы) и выберите команду **Все задачи** > **Удалить**.

3. Выберите метод удаления **Немедленно удалить программы из учетных записей пользователей и компьютеров**.

4. Примените изменения с помощью команды `gpupdate / force`.

Kaspersky Embedded Systems Security будет удален с защищаемых устройств после их перезагрузки, перед входом в Microsoft Windows.

Проверка функций Kaspersky Embedded Systems Security. Использование тестового вируса EICAR

В этом разделе описан тестовый вирус EICAR и его использование для проверки функций постоянной защиты файлов и проверки по требованию Kaspersky Embedded Systems Security.

О тестовом вирусе EICAR

Тестовый вирус предназначен для проверки работы антивирусных программ. Он разработан организацией The European Institute for Computer Antivirus Research (EICAR).

Тестовый вирус не является вредоносным объектом и не содержит исполняемого кода, который может нанести вред вашему устройству, но антивирусные программы большинства производителей идентифицируют его как угрозу.

Файл, который содержит тестовый вирус, называется eicar.com. Его можно загрузить на веб-сайте EICAR.

Перед сохранением файла в папку на жестком диске устройства убедитесь, что Постоянная защита файлов выключена для этого жесткого диска.

Файл eicar.com содержит текстовую строку. При проверке файла Kaspersky Embedded Systems Security обнаруживает в этой текстовой строке тестовую угрозу, присваивает файлу статус **Зараженный или обнаруживаемый** и удаляет его. Информация об обнаруженной в файле угрозе появляется в Консоли программы и в журнале выполнения задачи.

Вы также можете использовать файл eicar.com, чтобы проверять, как Kaspersky Embedded Systems Security выполняет лечение зараженных объектов и обнаруживает возможно зараженные объекты. Для этого откройте файл с помощью текстового редактора, добавьте к началу текстовой строки в файле один из префиксов, перечисленных в таблице ниже, и сохраните файл с новым именем, например, eicar_cure.com.

Чтобы убедиться, что Kaspersky Embedded Systems Security обрабатывает файл eicar.com с префиксом, в разделе параметров безопасности **Защита объектов** установите значение **Все объекты** для задач постоянной защиты компьютера и проверки по требованию в Kaspersky Embedded Systems Security.

Префиксы в файлах EICAR

Префикс	Статус файла после проверки и действие Kaspersky Embedded Systems Security
Без префикса	**Kaspersky Embedded Systems Security присваивает объекту статус Зараженный или обнаруживаемый и удаляет его.**

SUSP–	Kaspersky Embedded Systems Security присваивает статус **Возможно зараженный** объекту, обнаруженному с помощью эвристического анализатора, и удаляет его, поскольку возможно зараженные объекты не подвергаются лечению.
WARN–	Kaspersky Embedded Systems Security присваивает статус **Возможно зараженный** объекту, если код объекта частично совпадает с кодом известной угрозы, и удаляет его, поскольку возможно зараженные объекты не подвергаются лечению.
CURE–	Kaspersky Embedded Systems Security присваивает объекту статус **Зараженный или обнаруживаемый** и лечит его. Если лечение успешно, весь текст в файле заменяется словом "CURE".

Проверка функций постоянной защиты файлов и проверки по требованию

После установки Kaspersky Embedded Systems Security вы можете убедиться, что Kaspersky Embedded Systems Security обнаруживает объекты, содержащие вредоносный код. Для этого можно использовать тестовый вирус EICAR.

Чтобы проверить функцию постоянной защиты файлов, выполните следующие действия:

1. Загрузите файл eicar.com с веб-сайта EICAR. Сохраните его в папку общего доступа на локальном диске любого устройства сети.

   Перед сохранением файла в папку убедитесь, что функция постоянной защиты файлов отключена для этой папки.

2. Если вы хотите проверить работу уведомлений пользователей сети, убедитесь, что Служба сообщений Microsoft Windows включена на защищаемом устройстве и на устройстве, на котором сохранен файл eicar.com.

3. Откройте Консоль программы на защищаемом устройстве.

4. Скопируйте сохраненный файл eicar.com на локальный диск защищаемого устройства одним из следующих способов:

   - Чтобы проверить работу уведомлений через окно Службы терминалов, скопируйте файл eicar.com на защищаемое устройство, подключившись к защищаемому устройству с помощью программы "Подключение к удаленному рабочему столу" (Remote Desktop Connection).

   - Чтобы проверить работу уведомлений через Службу сообщений Microsoft Windows, скопируйте файл eicar.com с устройства, на котором вы его сохранили, через сетевое окружение этого устройства.

Постоянная защита файлов работает должным образом, если выполняются следующие условия:

- Файл eicar.com удален с защищаемого устройства.

- В Консоли программы журналу выполнения задачи присвоен статус *Критический*. В журнале появилась строка с информацией об угрозе в файле eicar.com. Чтобы просмотреть журнал выполнения задачи, в дереве Консоли программы разверните узел **Постоянная защита компьютера**, выберите задачу **Постоянная защита файлов** и в панели результатов узла перейдите по ссылке **Открыть журнал выполнения**.

- На устройстве, с которого вы скопировали файл, появилось следующее сообщение Службы сообщений Microsoft Windows: `Программа Kaspersky Embedded Systems Security заблокировала доступ к <путь к файлу eicar.com на устройстве>\eicar.com на компьютере <сетевое имя устройства> в <время возникновения события>. Причина: обнаружена угроза. Вирус: EICAR-Test-File. Имя пользователя: <имя пользователя>. Имя компьютера: <сетевое имя устройства, с которого вы скопировали файл>`.

Убедитесь, что Служба сообщений Microsoft Windows работает на устройстве, с которого вы скопировали файл eicar.com.

Чтобы проверить функцию проверки по требованию, выполните следующие действия:

1. Загрузите файл eicar.com с веб-сайта EICAR. Сохраните его в папку общего доступа на локальном диске любого устройства сети.

   Перед сохранением файла в папку убедитесь, что функция постоянной защиты файлов отключена для этой папки.

2. Откройте Консоль программы.

3. Выполните следующие действия:

   a. В дереве Консоли программы разверните узел **Проверка по требованию**.

   b. Выберите вложенный узел **Проверка важных областей**.

   c. На закладке **Настройка области проверки** откройте контекстное меню узла **Сетевое окружение** и выберите пункт **Добавить сетевой файл.**

   d. Введите сетевой путь к файлу eicar.com на удаленном устройстве в формате UNC (Universal Naming Convention).

   e. Установите флажок, чтобы включить добавленный сетевой путь в область проверки.

   f. Запустите задачу Проверка важных областей.

Проверка по требованию работает должным образом, если выполняются следующие условия:

- Файл eicar.com удален с жесткого диска устройства.
- В Консоли программы журналу выполнения задачи присвоен статус *Критический*. В журнале выполнения задачи проверки важных областей появилась строка с информацией об угрозе в файле eicar.com. Чтобы просмотреть журнал выполнения задачи, в дереве Консоли программы разверните узел **Проверка по требованию**, выберите задачу Проверка важных областей и в панели результатов перейдите по ссылке **Открыть журнал выполнения**.

Прочие ограничения

Проверка по требованию и **Постоянная защита файлов**:

- Проверка подключенных устройств, работающих по протоколу MTP, не поддерживается.
- Проверка архивов невозможна без проверки SFX-архивов: если проверка архивов включена в параметрах защиты Kaspersky Embedded Systems Security, программа автоматически проверяет объекты как в архивах, так и в SFX-архивах. Возможна проверка SFX-архивов без проверки архивов.

Лицензирование:

- В мастере установки не поддерживается активация программы с помощью файла ключа, если файл ключа хранится на диске, созданном с помощью команды SUBST, или если указан сетевой путь к файлу ключа.

Обновления:

- После установки критических обновлений модулей Kaspersky Embedded Systems Security, по умолчанию значок программы будет скрыт.
- KLRAMDISK не поддерживается на защищаемых устройствах с операционными системами Windows XP и Windows Server 2003.

Интерфейс:

- При использовании фильтров в Консоли программы учитывается регистр для карантина, резервного хранилища, журнала системного аудита и журналов выполнения задач.
- При настройке области защиты и области проверки в Консоли программы можно использовать только одну маску и только в конце пути. Примеры использования маски: "C:\Temp\Temp*", "C:\Temp\Temp???.doc", "C:\Temp\Temp*.doc". Это ограничение не распространяется на настройку доверенной зоны.

Безопасность:

- Если в операционной системе активирован Контроль учетных записей, учетные записи пользователей должны входить в группу администраторов KAVWSEE, чтобы можно было открывать Консоль программы двойным щелчком мыши на значке программы в области уведомлений панели задач. В противном случае для входа придется использовать учетную запись с правами открывать Диагностическое окно или оснастку Microsoft Management Console (MMC).
- Если активирован Контроль учетных записей пользователей, недоступно удаление программы из окна Microsoft Windows **Программы и компоненты**.

Интеграция с Kaspersky Security Center:

- Сервер администрирования проверяет обновления баз программы при получении пакетов обновлений, перед отправкой обновлений на защищаемые устройства сети. Сервер администрирования не проверяет обновления модулей программы.
- Убедитесь, что установлены необходимые флажки в окне параметров взаимодействия с Сервером администрирования, при использовании компонентов, передающих динамические данные в Kaspersky Security Center с помощью сетевых списков (карантин, резервное хранилище).

Защита от эксплойтов:

- Защита от эксплойтов недоступна, если библиотеки apphelp.dll не загружены в текущей конфигурации сетевого окружения.

- Компонент Защита от эксплойтов несовместим с утилитой EMET от Microsoft на защищаемых устройствах с операционной системой Microsoft Windows 10. Kaspersky Embedded Systems Security блокирует EMET, если компонент Защита от эксплойтов установлен на защищаемом устройстве с установленной утилитой EMET.

Интерфейс программы

Вы можете управлять Kaspersky Embedded Systems Security с помощью Плагина управления и через локальную Консоль программы.

Действия в интерфейсе локальной Консоли программы описаны в разделе Работа с Консолью программы.

Действия с Плагином управления осуществляются в интерфейсе Консоли администрирования Kaspersky Security Center. Подробная информация об интерфейсе Kaspersky Security Center приведена в *Справке Kaspersky Security Center*.

Лицензирование программы

Этот раздел содержит информацию об основных понятиях, связанных с лицензированием программы.

О Лицензионном соглашении

Лицензионное соглашение – это юридическое соглашение между вами и АО "Лаборатория Касперского", в котором указано, на каких условиях вы можете использовать программу.

Внимательно ознакомьтесь с условиями Лицензионного соглашения перед началом работы с программой.

Вы можете ознакомиться с условиями Лицензионного соглашения следующими способами:

- Во время установки Kaspersky Embedded Systems Security.
- Прочитав документ license.txt. Этот документ включен в комплект поставки программы.

Вы принимаете условия Лицензионного соглашения, подтверждая свое согласие с текстом Лицензионного соглашения во время установки программы. Если вы не согласны с условиями Лицензионного соглашения, вы должны прервать установку программы и не должны использовать программу.

О лицензии

Лицензия – это ограниченное по времени право на использование программы, предоставляемое вам на основе Лицензионного соглашения.

Лицензия включает в себя право на получение следующих видов услуг:

- использование программы в соответствии с условиями Лицензионного соглашения;
- получение технической поддержки.

Объем услуг и срок использования программы зависит от типа лицензии, используемой для активации программы.

Программа активируется с помощью файла ключа или кода активации для приобретенной коммерческой лицензии.

Коммерческая лицензия – платная лицензия, предоставляемая при приобретении программы.

В Kaspersky Embedded Systems Security предусмотрены следующие типы коммерческих лицензий:

- стандартная лицензия Kaspersky Embedded Systems Security;
- расширенная лицензия Kaspersky Embedded Systems Security Compliance Edition, распространяющаяся на два дополнительных компонента системы: Мониторинг файловых операций и Анализ журналов.

По истечении срока действия коммерческой лицензии программа продолжает работу, но с ограниченной функциональностью (например, недоступно обновление баз Kaspersky Embedded Systems Security). Чтобы продолжить использование Kaspersky Embedded Systems Security в режиме полной функциональности, вам нужно продлить срок действия коммерческой лицензии.

Рекомендуется продлевать срок действия лицензии не позднее даты его окончания, чтобы обеспечить максимальную защиту устройства от угроз компьютерной безопасности.

Убедитесь, что дата окончания срока действия дополнительного ключа наступает позже даты окончания срока действия активного ключа.

О Лицензионном сертификате

Лицензионный сертификат – это документ, который передается вам вместе с файлом ключа или кодом активации (если применимо).

В Лицензионном сертификате содержится следующая информация о предоставляемой лицензии:

- номер заказа;
- информация о пользователе, которому предоставлена лицензия;
- информация о программе, которую можно активировать по предоставляемой лицензии;
- ограничение количества лицензионных единиц (например, устройства, на которых можно использовать программу с предоставленной лицензией);
- дата начала срока действия лицензии;
- дата окончания срока действия лицензии или срок действия лицензии;
- тип лицензии.

О ключе

Ключ – последовательность бит, с помощью которой вы можете активировать и затем использовать программу в соответствии с условиями Лицензионного соглашения. Ключ создается специалистами "Лаборатории Касперского".

Вы можете добавить ключ в программу с помощью файла ключа. Ключ отображается в интерфейсе программы в виде уникальной буквенно-цифровой последовательности, после того как вы добавили его в программу.

Ключ может быть заблокирован "Лабораторией Касперского", если условия Лицензионного соглашения нарушены. Если ключ заблокирован, для работы программы требуется добавить другой ключ.

Ключ может быть активным и дополнительным.

Активный ключ – ключ, используемый в текущий момент для работы программы. В качестве активного может быть добавлен ключ для коммерческой или пробной лицензии. В программе не может быть больше одного активного ключа.

Дополнительный ключ – ключ, подтверждающий право на использование программы, но не используемый в текущий момент. Дополнительный ключ автоматически становится активным, когда заканчивается срок действия лицензии, связанной с текущим активным ключом. Дополнительный ключ может быть добавлен только при наличии активного ключа.

О файле ключа

Файл ключа – это файл с расширением key, который вам предоставляет "Лаборатория Касперского". Файл ключа предназначен для добавления лицензионного ключа, активирующего программу.

Вы получаете файл ключа на указанный вами адрес электронной почты после приобретения Kaspersky Embedded Systems Security или заказа пробной версии Kaspersky Embedded Systems Security.

Чтобы активировать программу с помощью файла ключа, не требуется подключение к серверам активации "Лаборатории Касперского".

Если файл ключа был случайно удален, вы можете его восстановить. Файл ключа может потребоваться вам, например, для регистрации Kaspersky CompanyAccount.

Для восстановления файла ключа выполните одно из следующих действий:

- Обратитесь к поставщику лицензии.
- Получите файл ключа на сайте "Лаборатории Касперского" с помощью имеющегося у вас кода активации.

О коде активации

Код активации – уникальная последовательность из 20 символов (букв и цифр). Вам нужно ввести код активации, чтобы добавить ключ для активации Kaspersky Embedded Systems Security. Вы получаете код активации на адрес электронной почты, указанный при приобретении Kaspersky Embedded Systems Security или при заказе пробной версии Kaspersky Embedded Systems Security.

Чтобы активировать программу с помощью кода активации, необходим доступ в интернет для подключения к серверам активации "Лаборатории Касперского".

Можно восстановить утерянный после установки программы код активации. Код активации может понадобиться, например, чтобы зарегистрировать Kaspersky CompanyAccount. Для восстановления кода активации обратитесь в Службу технической поддержки "Лаборатории Касперского".

О предоставлении данных

Лицензионное соглашение для Kaspersky Embedded Systems Security, в частности в разделе "Условия обработки данных", определяет условия, ответственность и порядок передачи и обработки данных, указанных в настоящем Руководстве. Внимательно ознакомьтесь с условиями Лицензионного соглашения, а также со всеми документами, ссылки на которые содержит Лицензионное соглашение, перед тем, как принять его.

Данные, которые "Лаборатория Касперского" получает от вас при использовании программы, защищаются и обрабатываются в соответствии с Политикой конфиденциальности, опубликованной на сайте: www.kaspersky.ru/Products-and-Services-Privacy-Policy.

Условия Лицензионного соглашения и Политики конфиденциальности доступны при установке Kaspersky Embedded Systems Security в составе комплекта поставки, а также из меню **Пуск** после установки программы (**Все программы** > **Kaspersky Embedded Systems Security** > **Лицензионное соглашение и Политика конфиденциальности**).

При удалении Kaspersky Embedded Systems Security будут удалены все данные Kaspersky Embedded Systems Security, хранящиеся на защищаемом устройстве.

Принимая условия Лицензионного соглашения, вы соглашаетесь отправлять в автоматическом режиме следующие данные в "Лабораторию Касперского":

- Для обеспечения механизма получения обновлений - информацию об установленной программе и активации программы: идентификатор устанавливаемой программы и ее полную версию, включая номер сборки, тип и идентификатор лицензии, идентификатор установки, идентификатор задачи обновления.
- Для использования возможности перехода на статьи Базы знаний при возникновении ошибок в работе программы (служба Redirector) – данные о программе и ссылке: название, локализацию и полный номер версии программы, тип перенаправляющей ссылки, а также идентификатор возникшей ошибки.
- Для контроля получения согласий на обработку данных – информацию о статусе согласия с условиями Лицензионного соглашения и других документов, регламентирующих отправку данных: идентификатор и версия Лицензионного соглашения или другого документа, в рамках которого выполняется согласие с условиями обработки данных или отзыв согласия; признак, указывающий на действие пользователя (подтверждение согласия с условиями или отзыв согласия); дата и время изменения статуса согласия с условиями обработки данных.

Локальная обработка данных

В процессе выполнения основных функций программы, описанных в настоящем Руководстве, Kaspersky Embedded Systems Security локально обрабатывает и хранит набор данных на защищаемом компьютере.

В следующей таблице содержится информация о локальной обработке и хранении программой Kaspersky Embedded Systems Security данных, содержащихся в отчетах.

Обработка и хранение данных, содержащихся в отчетах

Функциональная область	Запись событий
Тип использования	Kaspersky Embedded Systems Security хранит данные локально и передает данные на Сервер администрирования. В базе данных Сервера администрирования хранится информация о событиях программы, произошедших на управляемых защищаемых устройствах.
Хранилище	• %ALLUSERSPROFILE%\Kaspersky Lab\Kaspersky Embedded Systems Security\<версия продукта>\Reports • %SystemRoot%\System32\Winevt\Logs\Kaspersky Security.evtx • База данных Сервера администрирования

Меры безопасности	Список контроля доступа (Access-control list).
Период хранения	Kaspersky Embedded Systems Security хранит данные до момента удаления Kaspersky Embedded Systems Security. При удалении Kaspersky Embedded Systems Security будут удалены все данные Kaspersky Embedded Systems Security, хранящиеся на защищаемом устройстве.
Назначение	Обеспечение основных функций.

Kaspersky Embedded Systems Security не удаляет события в журнале событий Windows, в том числе события, произошедшие во время удаления Kaspersky Embedded Systems Security.

Чтобы обеспечить функцию регистрации событий, Kaspersky Embedded Systems Security локально обрабатывает следующие данные:

- Имена, контрольные суммы (MD5, SHA-256) и атрибуты обрабатываемых файлов и полные пути к ним на проверяемом носителе.
- Действия, выполняемые над проверяемыми файлами программой Kaspersky Embedded Systems Security.
- Действия, выполняемые пользователями над проверяемыми файлами на защищаемом компьютере.
- Информация об учетных записях пользователей, выполняющих действия в защищаемой сети или на защищаемом устройстве.
- Значения путей к экземплярам устройств, добавленных в правила контроля устройств.
- Информация о процессах и скриптах, запущенных в системе: контрольные суммы (MD5, SHA-256) и полные пути к исполняемым файлам, информация о цифровых сертификатах.
- Параметры брандмауэра Windows.
- Записи журнала событий Windows.
- Имена учетных записей пользователей, выполняющих действия над проверяемыми файлами на защищаемом компьютере.
- Экземпляры запущенных исполняемых файлов, а также типы, имена, контрольные суммы и атрибуты этих файлов.
- Информация о сетевой активности:
  - IP-адреса заблокированных внешних устройств.
  - Обработанные IP-адреса.
- Информация о статусе USN-журнала Windows.

В следующей таблице приведена информация о служебных данных, обрабатываемых Kaspersky Embedded Systems Security. Служебные данные включают: параметры программы, файлы на карантине и в резервном хранилище, информацию в сервисных базах данных программы, данные лицензирования.

В следующей таблице содержится информация о локальной обработке и хранении программой Kaspersky Embedded Systems Security данных о параметрах, указанных пользователями.

Функциональная область	Все функции Kaspersky Embedded Systems Security
Тип использования	Kaspersky Embedded Systems Security хранит данные локально и передает данные на Сервер администрирования. Данные хранятся в базе данных Сервера администрирования. Данные, обрабатываемые программой локально, не передаются автоматически в "Лабораторию Касперского" или другие сторонние системы.
Хранилище	• %ALLUSERSPROFILE%\Kaspersky Lab\Kaspersky Embedded Systems Security\<версия продукта>\ • База данных Сервера администрирования
Меры безопасности	Список контроля доступа (Access-control list).
Период обработки	Kaspersky Embedded Systems Security хранит данные до момента удаления Kaspersky Embedded Systems Security. При удалении Kaspersky Embedded Systems Security будут удалены все данные Kaspersky Embedded Systems Security, хранящиеся на защищаемом устройстве. Kaspersky Embedded Systems Security не удаляет данные о параметрах, экспортируемых в конфигурационный файл. Kaspersky Embedded Systems Security не удаляет объекты на карантине и в резервном хранилище, если в мастере установки были установлены флажки **Экспортировать объекты на карантине** и **Экспортировать объекты резервного хранилища**.
Назначение	Обеспечение основных функций.

Для заявленных целей Kaspersky Embedded Systems Security локально обрабатывает следующие данные:

- Объекты, помещенные на карантин и в резервное хранилище.
- Информация об учетных записях пользователей (имена пользователей и пароли), с правами которых запускаются задачи Kaspersky Embedded Systems Security.
- Пароль Kaspersky Embedded Systems Security.
- IP-адреса и идентификаторы заблокированных сеансов входа.
- Параметры брандмауэра Windows и параметры правил брандмауэра Windows.
- Контрольные суммы (MD5, SHA-256) и пути к исполняемым файлам, добавленным в правила задачи Контроль запуска программ.
- Значения путей к экземплярам устройств, добавленных в правила контроля устройств.
- Информация о файлах и папках, включенных в области задач Kaspersky Embedded Systems Security.
- IP-адреса, включенные или исключенные из области защиты.
- Информация о событиях в журнале событий Windows.
- Информация об объектах, обнаруженных с использованием технологий iSwift и iChecker.

- Контрольные суммы (MD5, SHA-256), полные пути и маски, указанные в параметрах исключений.
- Информация о процессах, добавленных в Доверенную зону.
- Информация о добавленных лицензионных ключах.
- Информация о цифровых сертификатах.
- Файлы, распакованные из архива или другого составного объекта во время проверки.

Kaspersky Embedded Systems Security обрабатывает и хранит данные в рамках основной функциональности программы, в том числе для регистрации событий программы и получения диагностических данных. Защита локально обрабатываемых данных выполняется в соответствии с настроенными и применяющимися параметрами программы.

Kaspersky Embedded Systems Security позволяет настроить уровень защиты данных, обрабатываемых локально (Управление правами доступа к функциям Kaspersky Embedded Systems Security, Регистрация событий. Журналы Kaspersky Security для Windows). Вы можете изменять права пользователей на доступ к обрабатываемым данным, изменять сроки хранения таких данных, частично или полностью отключать функциональность, в рамках которой выполняется регистрация данных, а также изменять путь к папке, в которую выполняется запись данных, и ее атрибуты.

Данные, обрабатываемые программой локально, не передаются автоматически в "Лабораторию Касперского" или другие сторонние системы.

По умолчанию все данные, локально обрабатываемые программой в ходе работы, удаляются после удаления Kaspersky Embedded Systems Security с защищаемого устройства.

Исключение составляют файлы с диагностической информацией (файлы трассировки и файлы дампов), файлы журнала событий Windows с событиями программы и файлы с экспортированными параметрами Kaspersky Embedded Systems Security. Рекомендуется самостоятельно удалить эти файлы.

Вы можете найти детальную информацию по работе с файлами, содержащими диагностические данные программы, в соответствующих разделах настоящего Руководства.

Вы можете удалить файлы журнала Windows с программными событиями Kaspersky Embedded Systems Security стандартными средствами операционной системы.

Локальная обработка данных вспомогательными компонентами программы

В пакет установки Kaspersky Embedded Systems Security включены вспомогательные компоненты программы, которые могут быть установлены на устройстве, даже если на нем не установлена программа Kaspersky Embedded Systems Security. К таким вспомогательным компонентам относятся:

- Консоль локального управления программой. Компонент входит в состав Средств администрирования Kaspersky Embedded Systems Security и представляет собой оснастку Microsoft Management Console.
- Плагин управления. Компонент обеспечивает полноценную интеграцию с программой Kaspersky Security Center.

При выполнении основных функций программы, описанных в настоящем Руководстве, вспомогательные компоненты программы локально обрабатывают и хранят набор данных на защищаемом устройстве, на котором они установлены, даже если они установлены отдельно от Kaspersky Embedded Systems Security.

Компоненты программы локально обрабатывают и хранят следующие данные:

- Консоль программы: имя защищаемого устройства с установленной программой Kaspersky Embedded Systems Security (IP-адрес или доменное имя), к которому в последний раз выполнялось удаленное подключение через Консоль программы; настроенные параметры отображения в оснастке Microsoft Management Console; данные о последней папке, в которой пользователь выполнял выбор объектов посредством Консоли программы (через системный диалог, открывающийся по кнопке **Обзор**). Файлы трассировки Консоли программы могут содержать следующие данные: имя защищаемого устройства с установленной программой Kaspersky Embedded Systems Security, к которому выполнялось удаленное подключение; имя учетной записи, с правами которой выполнялось удаленное подключение.

- Плагин управления может обрабатывать и временно хранить данные, обрабатываемые Kaspersky Embedded Systems Security, например, настроенные параметры задач и компонентов программы, параметры политик Kaspersky Security Center, данные, передаваемые в сетевых списках.

В следующей таблице содержится информация о локальной обработке и хранении программой Kaspersky Embedded Systems Security данных, записываемых в файлы дампов и файлы трассировки.

Kaspersky Embedded Systems Security локально обрабатывает и хранит следующие данные, записанные в файлы дампов и файлы трассировки:

- Информация о действиях, выполняемых программой Kaspersky Embedded Systems Security на защищаемом устройстве.

- Информация об объектах, обработанных программой Kaspersky Embedded Systems Security.

- Информация о действиях на защищаемом устройстве, обрабатываемая Kaspersky Embedded Systems Security.

- Информация об ошибках, возникших во время работы программы Kaspersky Embedded Systems Security.

Данные, обрабатываемые вспомогательными компонентами программы, не передаются автоматически в "Лабораторию Касперского" или другие сторонние системы.

По умолчанию все данные, локально обрабатываемые вспомогательными компонентами программы в ходе работы, удаляются после удаления этих компонентов.

Исключение составляют файлы трассировки вспомогательных компонентов программы. Рекомендуется самостоятельно удалить эти файлы.

Данные в файлах трассировки и файлах дампов

Kaspersky Embedded Systems Security в соответствии с заданными параметрами может записывать отладочную информацию в файлы трассировки в целях предоставления технической поддержки во время работы Kaspersky Embedded Systems Security.

Файлы дампов программы Kaspersky Embedded Systems Security формируются операционной системой во время сбоев программы и перезаписываются при следующем сбое.

Файлы трассировки и дампов могут содержать персональные данные пользователей или конфиденциальные данные организации.

Не используйте Kaspersky Embedded Systems Security на устройствах, для которых передача данных запрещена политикой организации.

По умолчанию Kaspersky Embedded Systems Security не записывает отладочную информацию.

Файлы трассировки и дампов не отправляются автоматически за пределы устройства, на котором они были сформированы. Содержимое файлов трассировки можно просматривать с помощью стандартных средств просмотра текстовых файлов. Файлы трассировки и дампов хранятся неограниченное время и не удаляются при удалении Kaspersky Embedded Systems Security.

Отладочная информация может быть полезна для технической поддержки.

Для ограничения доступа к файлам трассировки и дампов никаких специальных механизмов не предусмотрено. Администратор может настроить запись этих данных в защищенную папку.

Путь к папке с файлами трассировки и дампов по умолчанию не задан. Администратор должен указать папку трассировки и дампов, чтобы использовать ее.

В файлах трассировки и дампов могут содержаться следующие данные:

- Информация о действиях, выполняемых программой Kaspersky Embedded Systems Security на защищаемом устройстве.
- Информация об объектах, обработанных Kaspersky Endpoint Agent.
- Информация об ошибках, возникающих при работе Kaspersky Endpoint Agent.

Активация программы с помощью файла ключа

Вы можете активировать Kaspersky Embedded Systems Security с помощью файла ключа.

Если в Kaspersky Embedded Systems Security уже добавлен активный ключ и вы добавите другой ключ в качестве активного, то новый ключ заменит ранее добавленный ключ. Добавленный ранее ключ будет удален.

Если в Kaspersky Embedded Systems Security уже добавлен дополнительный ключ и вы добавите другой ключ в качестве дополнительного, то новый ключ заменит ранее добавленный ключ. Добавленный ранее дополнительный ключ будет удален.

Если в Kaspersky Embedded Systems Security уже добавлены активный ключ и дополнительный ключ, а вы добавите новый ключ в качестве активного, то новый ключ заменит ранее добавленный активный ключ, а дополнительный ключ не будет удален.

Чтобы активировать Kaspersky Embedded Systems Security с помощью файла ключа, выполните следующие действия:

1. В дереве Консоли программы разверните узел **Лицензирование**.
2. В панели результатов узла **Лицензирование** перейдите по ссылке **Добавить ключ**.
3. В открывшемся окне нажмите на кнопку **Обзор**.
4. Выберите файл ключа с расширением key.

   Вы также можете добавить ключ в качестве дополнительного. Для этого установите флажок **Использовать в качестве дополнительного ключа**.

5. Нажмите на кнопку **ОК**.

Будет применен выбранный файл ключа. Информация о добавленном ключе отобразится в панели результатов узла **Лицензирование**.

Активация программы с помощью кода активации

Для активации программы с помощью кода активации защищаемое устройство должно быть подключено к интернету.

Вы можете активировать Kaspersky Embedded Systems Security с помощью кода активации.

При активации этим способом Kaspersky Embedded Systems Security отправляет данные на сервер активации для проверки введенного кода:

- В случае успешной проверки кода активации программа будет активирована.
- При сбое проверки кода активации отобразится соответствующее уведомление. В этом случае обратитесь к поставщику, у которого была приобретена лицензия на программу Kaspersky Embedded Systems Security.
- В случае превышения количества активаций с помощью указанного кода активации, отображается соответствующее уведомление. Процесс активации программы будет прерван, и вам будет предложено обратиться в Службу технической поддержки "Лаборатории Касперского".

Чтобы активировать Kaspersky Embedded Systems Security с помощью кода активации, выполните следующие действия:

1. В дереве Консоли программы разверните узел **Лицензирование**.
2. В панели результатов узла **Лицензирование** перейдите по ссылке **Добавить код активации**.
3. В открывшемся окне введите код активации в поле **Код активации**.
   - Чтобы применить код активации для добавления дополнительного ключа, установите флажок **Использовать в качестве дополнительного ключа**.
   - Чтобы просмотреть информацию о лицензии, нажмите на кнопку **Показать информацию о лицензии**. Информация отобразится в блоке **Информация о лицензии**.
4. Нажмите на кнопку **ОК**.

   Kaspersky Embedded Systems Security отправит информацию о примененном коде активации на сервер активации.

Просмотр информации о действующей лицензии

Просмотр информации о лицензии

Информация о действующей лицензии отображается в панели результатов узла **Kaspersky Embedded Systems Security** Консоли программы. Ключ может иметь один из следующих статусов:

- **Выполняется проверка статуса лицензии** – программа Kaspersky Embedded Systems Security проверяет примененный файл ключа или код активации и ожидает ответа о текущем статусе ключа.
- **Дата окончания срока действия лицензии** – программа Kaspersky Embedded Systems Security активирована до указанной даты и времени. Статус ключа выделен желтым цветом в следующих случаях:
  - До истечения срока действия лицензии остается не более 14 дней, и не добавлен дополнительный ключ.
  - Добавленный ключ помещен в черный список и будет заблокирован.
- **Срок действия лицензии истек** – программа Kaspersky Embedded Systems Security не активирована, поскольку истек срок действия лицензии. Статус выделен красным цветом.
- **Нарушено Лицензионное соглашение** – программа Kaspersky Embedded Systems Security не активирована, поскольку нарушены условия Лицензионного соглашения. Статус выделен красным цветом.
- **Ключ помещен в черный список** – добавленный ключ заблокирован и помещен в черный список специалистами "Лаборатории Касперского", например, если ключ был использован сторонними лицами для незаконной активации программы. Статус выделен красным цветом.

Просмотр информации о действующей лицензии

Чтобы просмотреть информацию о действующей лицензии,

в дереве Консоли программы разверните узел **Лицензирование**.

В панели результатов узла **Лицензирование** отобразится общая информация о действующей лицензии (см. таблицу ниже).

Общая информация о лицензии в узле Лицензирование

Поле	Описание
Код активации	Код активации. Поле заполняется, если вы активируете программу с помощью кода активации.
Статус активации	Информация о статусе активации программы. В графе **Статус активации** в панели результатов узла **Лицензирование** могут отображаться следующие значения: • **Применено** – если вы активировали программу с помощью кода активации или файла ключа. • **Активация** – если вы применили код активации для активации программы и процесс активации еще не закончен. Статус изменяется на **Применено** после завершения активации программы и обновления содержимого панели результатов узла. • **Ошибка активации** – если не удалось активировать программу. Вы можете посмотреть причину неудачного завершения активации в журнале выполнения задач.
Ключ	Ключ, добавленный для активации программы.
Тип лицензии	Тип лицензии: коммерческая или пробная.
Дата окончания	Дата и время окончания срока действия лицензии, связанной с активным ключом.

срока действия	
Статус кода активации или ключа	Статус кода активации или ключа: *Активный* или *Дополнительный*.

Чтобы просмотреть подробную информацию о лицензии,

в панели результатов узла **Лицензирование** в контекстном меню строки с информацией о лицензии, которую вы хотите просмотреть, выберите пункт **Свойства**.

В окне **Свойства ключа** на закладке **Общие** отображается подробная информация о действующей лицензии, а на закладке **Дополнительно** – информация о заказчике и контактная информация "Лаборатории Касперского" или партнера, у которого вы приобрели Kaspersky Embedded Systems Security (см. таблицу ниже).

Подробная информация о лицензии в окне Свойства: <Статус кода активации или ключа>

Поле	Описание
Закладка Общие	
Ключ	Ключ, добавленный для активации программы.
Дата добавления ключа	Дата добавления ключа в программу.
Тип лицензии	Тип лицензии: коммерческая или пробная.
Истекает через (сут)	Количество дней, оставшихся до окончания срока действия лицензии, связанной с активным ключом.
Дата окончания срока действия	Дата и время окончания срока действия лицензии, связанной с активным ключом. Если вы активируете программу по неограниченной подписке, в поле указывается значение *Не ограничена*. Если программе Kaspersky Embedded Systems Security не удается определить дату окончания действия лицензии, указывается значение *Неизвестна*.
Программа	Название программы, активированной с помощью файла ключа или кода активации.
Ограничение на использование ключа	Ограничение на использование ключа (если есть).
Осуществление технической поддержки	Информация о том, оказывает ли "Лаборатория Касперского" или ее партнеры техническую поддержку по условиям Лицензионного соглашения.
Закладка Дополнительно	
Информация о лицензии	Текущий лицензионный ключ.
Информация о поддержке	Контактная информация "Лаборатории Касперского" или партнера, который осуществляет техническую поддержку. Поле может быть пустым, если техническая поддержка не осуществляется.
Информация о владельце	Информация о владельце лицензии: имя клиента и название организации, для которой приобретена лицензия.

Функциональные ограничения после окончания срока действия лицензии

Когда заканчивается срок действия текущей лицензии, возникают следующие ограничения в работе функциональных компонентов:

- Останавливаются все задачи, за исключением задач Постоянная защита файлов, Проверка по требованию и Проверка целостности программы.
- Невозможно запустить ни одну задачу, кроме задач Постоянная защита файлов, Проверка по требованию и Проверка целостности программы. Эти задачи продолжат работать с использованием старых антивирусных баз.
- Функция Защита от эксплойтов ограничена:
  - Процессы защищаются до их перезапуска.
  - Новые процессы нельзя включить в область защиты.

Другие функции (хранилища, журналы, диагностические данные) по-прежнему доступны.

Продление срока действия лицензии

По умолчанию Kaspersky Embedded Systems Security уведомляет вас о скором окончании срока действия лицензии за 14 дней до окончания срока действия лицензии. При этом поле **Дата окончания срока действия лицензии** в панели результатов узла **Kaspersky Embedded Systems Security** выделяется желтым цветом.

Вы можете продлить срок действия лицензии, не дожидаясь его окончания, с помощью дополнительного ключа. Это позволяет не прерывать защиту устройства на период после окончания срока действия лицензии и до активации программы по новой лицензии.

Чтобы обновить лицензию, выполните следующие действия:

1. Получите новый файл ключа или код активации.
2. В дереве Консоли программы выберите узел **Лицензирование**.
3. В панели результатов узла **Лицензирование** выполните одно из следующих действий:
   - Если вы хотите продлить срок действия лицензии с помощью файла ключа:
     a. Перейдите по ссылке **Добавить ключ**.
     b. В открывшемся окне нажмите на кнопку **Обзор**.
     c. Выберите новый файл ключа с расширением key.
     d. Установите флажок **Использовать в качестве дополнительного ключа**.
   - Если вы хотите продлить срок действия лицензии с помощью кода активации:
     a. Перейдите по ссылке **Добавить код активации**.

b. В открывшемся окне введите приобретенный код активации.

c. Установите флажок **Использовать в качестве дополнительного кода активации**.

Для применения кода активации необходимо подключение к интернету.

4. Нажмите на кнопку **OK**.

Дополнительный ключ будет добавлен и автоматически станет активным по истечении срока действия текущей лицензии на Kaspersky Embedded Systems Security.

Удаление ключа

Вы можете удалить добавленный ключ из программы.

Если в Kaspersky Embedded Systems Security добавлен дополнительный ключ, и вы удалите активный ключ, дополнительный ключ автоматически станет активным.

Если вы удалите добавленный ключ, вы можете его восстановить, повторно применив файл ключа.

Чтобы удалить добавленный ключ, выполните следующие действия:

1. В дереве Консоли программы выберите узел **Лицензирование**.
2. В панели результатов узла **Лицензирование** в таблице с информацией о добавленных ключах выберите ключ, который вы хотите удалить.
3. В контекстном меню строки с информацией о выбранном ключе выберите пункт **Удалить**.
4. В окне подтверждения нажмите на кнопку **Да**, чтобы подтвердить удаление ключа.

Выбранный ключ будет удален.

Работа с Плагином управления

Этот раздел содержит информацию о Плагине управления Kaspersky Embedded Systems Security и об управлении программой, установленной на защищаемом устройстве или группе защищаемых устройств.

Управление Kaspersky Embedded Systems Security из Kaspersky Security Center

Вы можете централизованно управлять несколькими защищаемыми устройствами с установленной программой Kaspersky Embedded Systems Security, объединенными в группу администрирования, с помощью Плагина управления Kaspersky Embedded Systems Security. Kaspersky Security Center также позволяет отдельно настраивать параметры работы для каждого защищаемого устройства, входящего в группу администрирования.

Группа администрирования формируется вручную на стороне Kaspersky Security Center и включает несколько устройств с установленной программой Kaspersky Embedded Systems Security, для которых вы хотите настроить единые параметры управления и защиты. Подробная информация об использовании групп администрирования приведена в *Справке Kaspersky Security Center*.

Параметры программы для отдельного защищаемого устройства недоступны для настройки, если работа Kaspersky Embedded Systems Security на этом защищаемом устройстве контролируется активной политикой Kaspersky Security Center.

Вы можете управлять Kaspersky Embedded Systems Security из Kaspersky Security Center следующими способами:

- **С помощью политик Kaspersky Security Center**. Политики Kaspersky Security Center позволяют удаленно настроить единые параметры защиты для группы устройств. Параметры задачи, указанные в активной политике, имеют приоритет над параметрами задачи, настроенными локально в Консоли программы или удаленно в окне **Свойства: <Имя защищаемого устройства>** в Kaspersky Security Center.

  С помощью политик вы можете настроить общие параметры работы программы, параметры задач постоянной защиты, контроля активности на компьютерах, а также параметры запуска системных задач по расписанию.

- **С помощью групповых задач Kaspersky Security Center**. Групповые задачи Kaspersky Security Center позволяют удаленно настраивать единые параметры задач, имеющих ограниченный срок выполнения, для группы устройств.

- С помощью групповых задач вы можете активировать программу, настроить параметры задач проверки по требованию, параметры задач обновления и параметры задачи формирования правил контроля запуска программ.

- **С помощью задач для набора устройств**. Задачи для набора устройств позволяют удаленно настраивать единые параметры задач, имеющих ограниченный срок выполнения, для защищаемых устройств, не входящих ни в одну группу администрирования.

- **С помощью окна свойств отдельного компьютера**. В окне **Свойства: <Имя защищаемого устройства>** можно удаленно настроить параметры задачи для отдельного защищаемого устройства, включенного в группу администрирования. Вы можете настроить как общие параметры работы программы, так и параметры работы всех задач Kaspersky Embedded Systems Security, если выбранное защищаемое устройство не находится под управлением активной политики Kaspersky Security Center.

Kaspersky Security Center позволяет настроить параметры программы, дополнительные возможности и работу журналов и уведомлений. Вы можете настроить эти параметры как для группы защищаемых устройств, так и для отдельного защищаемого устройства.

Управление параметрами программы

Этот раздел содержит информацию о настройке общих параметров работы Kaspersky Embedded Systems Security в Kaspersky Security Center Web Console.

Навигация

В этом разделе описан переход к требуемым параметрам задачи с помощью интерфейса.

Переход к общим параметрам из политики

Чтобы открыть параметры программы Kaspersky Embedded Systems Security из политики, выполните следующие действия:

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой вы хотите настроить задачу.
3. Выберите закладку **Политики**.
4. Откройте окно свойств политики двойным щелчком мыши на имени политики, которую вы хотите настроить.
5. В открывшемся окне **Свойства: <Имя политики>** перейдите в раздел **Параметры программы**.
6. Нажмите на кнопку **Настройка** для группы параметров, которую вы хотите настроить.

Переход к общим параметрам из окна свойств программы

Чтобы открыть окно свойств Kaspersky Embedded Systems Security для отдельного защищаемого устройства, выполните следующие действия:

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой вы хотите настроить задачу.
3. Выберите закладку **Устройства**.
4. Откройте окно **Свойства: <Имя защищаемого устройства>** одним из следующих способов:
   - двойным щелчком мыши на имени защищаемого устройства;

- выбрав пункт **Свойства** в контекстном меню защищаемого устройства.

Откроется окно **Свойства: <Имя защищаемого устройства>**.

5. В разделе **Программы** выберите **Kaspersky Embedded Systems Security**.
6. Нажмите на кнопку **Свойства**.

   Откроется окно **Параметры Kaspersky Embedded Systems Security**.
7. Перейдите в раздел **Параметры программы**.

Настройка общих параметров программы в Kaspersky Security Center

Вы можете настроить общие параметры Kaspersky Embedded Systems Security из Kaspersky Security Center для группы защищаемых устройств или для отдельного защищаемого устройства.

Настройка масштабируемости и интерфейса в Kaspersky Security Center

Чтобы настроить параметры масштабируемости и интерфейс программы, выполните следующие действия:

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить параметры программы.
3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
   - Чтобы настроить параметры программы для группы защищаемых устройств, выберите закладку **Политики** и откройте окно **Свойства: <Имя политики>**.
   - Чтобы настроить параметры программы для отдельного защищаемого устройства, выберите закладку **Устройства** и откройте окно **Параметры программы**.

     Если к устройству применяется активная политика Kaspersky Security Center, запрещающая изменение параметров программы, эти параметры недоступны для изменения в окне **Параметры программы**.
4. В разделе **Параметры программы** в подразделе **Масштабируемость и интерфейс** нажмите на кнопку **Настройка**.
5. В окне **Дополнительные параметры программы** на закладке **Общие** настройте следующие параметры:
   - В разделе **Параметры масштабируемости** настройте параметры, определяющие количество процессов, которые использует Kaspersky Embedded Systems Security:
     - **Определять параметры масштабируемости автоматически**
     - **Указать количество рабочих процессов вручную**

- Максимальное количество активных процессов
- Количество процессов для постоянной защиты
- Количество процессов для фоновых задач проверки по требованию

- В разделе **Взаимодействие с пользователем** настройте отображение Значка области уведомлений в панели задач: снимите или установите флажок **Показывать Значок области уведомлений**.

6. На закладке **Иерархическое хранилище** выберите вариант доступа к иерархическому хранилищу.
7. Нажмите на кнопку **OK**.

Настроенные параметры программы будут сохранены.

Настройка параметров безопасности в Kaspersky Security Center

Чтобы настроить параметры безопасности вручную, выполните следующие действия:

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить параметры программы.
3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
   - Чтобы настроить параметры программы для группы защищаемых устройств, выберите закладку **Политики** и откройте окно **Свойства: <Имя политики>**.
   - Чтобы настроить параметры программы для отдельного защищаемого устройства, выберите закладку **Устройства** и откройте окно **Параметры программы**.

     Если к устройству применяется активная политика Kaspersky Security Center, запрещающая изменение параметров программы, эти параметры недоступны для изменения в окне **Параметры программы**.
4. В разделе **Параметры программы** в подразделе **Безопасность** нажмите на кнопку **Настройка**.
5. В окне **Параметры безопасности** настройте следующие параметры:
   - В разделе **Параметры надежности** настройте параметры восстановления задач Kaspersky Embedded Systems Security в случае сбоев в работе программы или аварийного завершения работы программы.
     - Выполнять восстановление задач
     - Выполнять восстановление задач проверки по требованию не более (раз)
   - В разделе **Действия при переходе на источник бесперебойного питания** задайте ограничение нагрузки на защищаемое устройство со стороны Kaspersky Embedded Systems Security при переходе на источник бесперебойного питания:
     - Не запускать задачи проверки по расписанию

- Остановить выполняемые задачи проверки

- В разделе **Параметры применения пароля** задайте пароль для защиты доступа к функциям Kaspersky Embedded Systems Security.

6. Нажмите на кнопку **OK**.

Настроенные параметры безопасности и надежности будут сохранены.

Настройка параметров соединения в Kaspersky Security Center

Настроенные параметры соединения используются для подключения Kaspersky Embedded Systems Security к серверам обновлений и активации, а также при интеграции программ со службами KSN.

Чтобы настроить параметры соединения, выполните следующие действия:

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.

2. Выберите группу администрирования, для которой требуется настроить параметры программы.

3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:

   - Чтобы настроить параметры программы для группы защищаемых устройств, выберите закладку **Политики** и откройте окно **Свойства: <Имя политики>**.

   - Чтобы настроить параметры программы для отдельного защищаемого устройства, выберите закладку **Устройства** и откройте окно **Параметры программы**.

     Если к устройству применяется активная политика Kaspersky Security Center, запрещающая изменение параметров программы, эти параметры недоступны для изменения в окне **Параметры программы**.

4. В разделе **Параметры программы** в подразделе **Параметры соединения** нажмите на кнопку **Настройка**.

   Откроется окно **Параметры соединения**.

5. В окне **Параметры соединения** настройте следующие параметры:

   - В разделе **Параметры прокси-сервера** задайте параметры использования прокси-сервера:

     - Не использовать прокси-сервер

     - Использовать параметры указанного прокси-сервера

     - IP-адрес или символьное имя прокси-сервера и номер порта

     - Не использовать прокси-сервер для локальных адресов

   - В разделе **Параметры аутентификации на прокси-сервере** задайте параметры аутентификации:

     - Выберите параметры аутентификации в раскрывающемся списке.

- **Не использовать аутентификацию** – проверка подлинности не производится. Этот режим выбран по умолчанию.
- **Использовать NTLM-аутентификацию** – проверка подлинности с помощью протокола сетевой аутентификации NTLM, разработанного компанией Microsoft.
- **Использовать NTLM-аутентификацию с именем пользователя и паролем** – проверка подлинности по протоколу сетевой аутентификации NTLM, разработанному компанией Microsoft, с использованием имени пользователя и пароля.
- **Использовать имя пользователя и пароль** – проверка подлинности с помощью имени пользователя и пароля.

- Если требуется, укажите имя пользователя и пароль.

- В разделе **Лицензирование** установите или снимите флажок **Использовать Kaspersky Security Center в качестве прокси-сервера для активации программы**.

6. Нажмите на кнопку **ОК**.

Настроенные параметры соединения будут сохранены.

Настройка запуска по расписанию локальных системных задач

С помощью политик можно разрешать или запрещать запуск локальных системных задач проверки по требованию и обновления по расписанию, настроенному локально на каждом защищаемом устройстве группы администрирования:

- Если запуск по расписанию для локальных системных задач указанных типов запрещен в политике, такие задачи не будут выполняться на защищаемом устройстве по расписанию. Вы можете запустить локальные системные задачи вручную.
- Если запуск по расписанию для локальных системных задач указанного типа разрешен в политике, такие задачи будут выполняться в соответствии с параметрами расписания, настроенными локально для этой задачи.

По умолчанию запуск локальных системных задач запрещается политикой.

Рекомендуется не разрешать запуск локальных системных задач, если обновления или проверки по требованию регулируются с помощью групповых задач Kaspersky Security Center.

Если вы не используете групповые задачи обновления или проверки по требованию, разрешите запуск локальных системных задач в политике: Kaspersky Embedded Systems Security будет выполнять обновления баз и модулей программы, а также запускать все локальные системные задачи проверки по требованию в соответствии с определенным по умолчанию расписанием.

С помощью политик вы можете разрешать или запрещать запуск по расписанию для следующих локальных системных задач:

- Задачи проверки по требованию: Проверка важных областей, Проверка объектов на карантине, Проверка при старте операционной системы, Проверка целостности программы, Мониторинг целостности файлов на основе эталона.

- Задачи обновления: Обновление баз программы, Обновление модулей программы, Копирование обновлений.

Если вы исключите защищаемое устройство из группы администрирования, расписание системных задач будет автоматически включено.

Чтобы разрешить или запретить в политике запуск по расписанию системных задач Kaspersky Embedded Systems Security, выполните следующие действия:

1. В дереве Консоли администрирования разверните узел **Управляемые устройства**, разверните нужную группу и в панели результатов выберите закладку **Политики**.
2. На закладке **Политики** в контекстном меню политики, для которой вы хотите настроить запуск по расписанию системных задач Kaspersky Embedded Systems Security для группы защищаемых устройств, выберите пункт **Свойства**.
3. В окне **Свойства: <Имя политики>** выберите раздел **Параметры программы**. В подразделе **Запуск системных задач** нажмите на кнопку **Настройка** и выполните одно из следующих действий:
   - Установите флажки **Разрешить запуск задач проверки по требованию** и **Разрешить запуск задач обновления и копирования обновлений**, чтобы разрешить запуск по расписанию перечисленных задач.
   - Снимите флажки **Разрешить запуск задач проверки по требованию** и **Разрешить запуск задач обновления и копирования обновлений**, чтобы запретить запуск по расписанию перечисленных задач.

   Установка или снятие флажков не влияет на параметры запуска локальных пользовательских задач указанного типа.
4. Убедитесь, что настраиваемая политика активна и применена к выбранной группе защищаемых устройств.
5. Нажмите на кнопку **OK**.

Настроенные параметры запуска по расписанию для выбранных задач будут применены.

Настройка параметров карантина и резервного хранилища в Kaspersky Security Center

Чтобы настроить параметры резервного хранилища в Kaspersky Security Center, выполните следующие действия:

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить параметры программы.
3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
   - Чтобы настроить параметры программы для группы защищаемых устройств, выберите закладку **Политики** и откройте окно **Свойства: <Имя политики>**.

- Чтобы настроить параметры программы для отдельного защищаемого устройства, выберите закладку **Устройства** и откройте окно **Параметры программы**.

  Если к устройству применяется активная политика Kaspersky Security Center, запрещающая изменение параметров программы, эти параметры недоступны для изменения в окне **Параметры программы**.

4. В разделе **Дополнительные возможности** нажмите на кнопку **Настройка** в подразделе **Хранилища**.

5. В окне **Параметры хранилищ** на закладке **Резервное хранилище** настройте следующие параметры резервного хранилища:

   - Чтобы задать папку резервного хранилища, в поле **Папка резервного хранилища** выберите нужную папку на локальном диске защищаемого устройства или введите полный путь к ней.

   - Чтобы задать максимальный размер резервного хранилища, установите флажок **Максимальный размер резервного хранилища (МБ)** и в поле ввода укажите нужное значение параметра в мегабайтах.

   - Чтобы задать порог свободного места в резервном хранилище, задайте значение для параметра **Максимальный размер резервного хранилища (МБ)**, установите флажок **Порог доступного пространства (МБ)** и укажите минимальный размер свободного места в папке резервного хранилища в мегабайтах.

   - Чтобы задать папку для восстановленных объектов, в разделе **Параметры восстановления объектов** выберите нужную папку на локальном диске защищаемого устройства или введите имя папки и полный путь к ней в поле **Папка, в которую восстанавливаются объекты**.

6. В окне **Параметры хранилищ** на закладке **Карантин** настройте следующие параметры карантина:

   - Чтобы изменить папку карантина, в поле **Папка карантина** укажите полный путь к папке на локальном диске защищаемого устройства.

   - Чтобы задать максимальный размер карантина, установите флажок **Максимальный размер карантина (МБ)** и в поле ввода укажите значение параметра в мегабайтах.

   - Чтобы задать минимальный объем свободного места в карантине, установите флажки **Максимальный размер карантина (МБ)** и **Порог доступного пространства (МБ)**, затем в поле ввода укажите значение в мегабайтах.

   - Чтобы изменить папку, в которую восстанавливаются объекты из карантина, в поле **Папка, в которую восстанавливаются объекты** укажите полный путь к папке на локальном диске защищаемого устройства.

7. Нажмите на кнопку **OK**.

Настроенные параметры карантина и резервного хранилища будут сохранены.

Создание и настройка политик

В этом разделе содержится информация о применении политик Kaspersky Security Center для управления Kaspersky Embedded Systems Security на нескольких защищаемых устройствах.

Можно создавать единые политики Kaspersky Security Center для управления защитой нескольких устройств, на которых установлена программа Kaspersky Embedded Systems Security.

Политика применяет указанные в ней значения параметров, функций и задач Kaspersky Embedded Systems Security на всех защищаемых устройствах одной группы администрирования.

Вы можете создать несколько политик для одной группы администрирования и применять их попеременно. Политика, действующая в группе в текущий момент, в Консоли администрирования имеет *активный* статус.

Информация о применении политики регистрируется в журнале системного аудита Kaspersky Embedded Systems Security. Вы можете просмотреть эту информацию в Консоли программы в узле **Журнал системного аудита**.

В Kaspersky Security Center существует единственный способ применения политик на защищаемых устройствах: *Запретить изменение параметров*. После применения политики Kaspersky Embedded Systems Security использует на защищаемых устройствах значения параметров, для которых в свойствах политики вы установили значок , вместо значений параметров, действующих до применения политики. Kaspersky Embedded Systems Security не применяет значения параметров активной политики, для которых в свойствах политики установлен значок .

Если политика активна, то значения параметров, отмеченные в политике значком , отображаются в Консоли программы, но недоступны для редактирования. Значения остальных параметров (отмеченных в политике значком) доступны для редактирования в Консоли программы.

Параметры, настроенные в активной политике и отмеченные значком , также блокируют изменение параметров в окне **Свойства: <Имя защищаемого устройства>** Kaspersky Security Center для отдельного защищаемого устройства.

Параметры, настроенные и переданные на защищаемое устройство с помощью активной политики, сохраняются в параметрах локальных задач после прекращения действия активной политики.

Если политика определяет параметры какой-либо из задач постоянной защиты компьютера и эта задача выполняется, параметры, определенные политикой, изменяются сразу после применения политики. Если задача не выполняется, параметры будут применены при ее запуске.

Создание политики

Создание новой политики состоит из следующих этапов:

1. Создание политики с помощью мастера создания политик. В окнах мастера можно настроить параметры задач постоянной защиты компьютера.

2. Настройка параметров политики. В окне **Свойства: <Имя политики>** созданной политики вы можете настроить параметры задач постоянной защиты компьютера, общие параметры Kaspersky Embedded Systems Security, параметры карантина и резервного хранилища, уровень детализации для журналов выполнения задач, уведомления пользователей и администратора о событиях Kaspersky Embedded Systems Security.

Чтобы создать политику для группы защищаемых устройств, на которых установлена и запущена программа Kaspersky Embedded Systems Security, выполните следующие действия:

1. В дереве Консоли администрирования Kaspersky Security Center разверните узел **Управляемые устройства** и выберите группу администрирования, для защищаемых устройств которой вы хотите

создать политику.

2. В панели результатов выбранной группы администрирования выберите закладку **Политики** и откройте окно мастера создания политик по ссылке **Создать политику**.

   Откроется окно **Мастер создания политики**.

3. В окне **Выбор программы для создания групповой политики** выберите Kaspersky Embedded Systems Security и нажмите на кнопку **Далее**.

4. В поле **Имя** укажите название групповой политики.

   Имя политики не должно содержать следующие символы: `" * < : > ? \ | .`

5. Чтобы применить параметры политики, используемые в предыдущей версии программы, выполните следующие действия:

   a. Установите флажок **Использовать параметры политики, созданной для предыдущей версии программы**.

   b. Нажмите на кнопку **Выбрать**.

   c. Выберите политику, которую требуется применить.

   d. Нажмите на кнопку **Далее**.

6. В окне **Выбор типа операции** выберите один из следующих вариантов:

   - **Создать**, чтобы создать политику с заданными по умолчанию параметрами.
   - **Импортировать политику, созданную с помощью Kaspersky Embedded Systems Security 3**, чтобы использовать импортированную версию политики в качестве шаблона.
   - Нажмите на кнопку **Обзор** и выберите конфигурационный файл, в который вы сохранили параметры ранее созданной политики.

7. В окне **Постоянная защита компьютера** настройте задачи и компоненты Постоянная защита файлов, Использование KSN, Защита от эксплойтов и Проверка скриптов. Разрешите или запретите применение настроенных задач политики на защищаемых устройствах сети:

   - Нажмите на кнопку , чтобы разрешить настройку параметров задачи на защищаемых устройствах сети и запретить применение настроенных в политике параметров задачи.
   - Нажмите на кнопку , чтобы запретить настройку параметров задачи на защищаемых устройствах сети и разрешить применение настроенных в политике параметров задачи.

   В созданной политике используются заданные по умолчанию параметры задач постоянной защиты компьютера.

   - Чтобы изменить заданные по умолчанию параметры задачи Постоянная защита файлов, нажмите на кнопку **Настройка** в подразделе **Постоянная защита файлов**. В открывшемся окне настройте параметры задачи в соответствии с вашими требованиями. Нажмите на кнопку **ОК**.
   - Чтобы изменить заданные по умолчанию параметры задачи Использование KSN, нажмите на кнопку **Настройка** в подразделе **Использование KSN**. В открывшемся окне настройте параметры задачи в соответствии с вашими требованиями. Нажмите на кнопку **ОК**.

Чтобы запустить задачу Использование KSN, необходимо принять Положение о KSN в окне Обработка данных в KSN.

- Чтобы изменить заданные по умолчанию параметры компонента Защита от эксплойтов, нажмите на кнопку **Настройка** в подразделе **Защита от эксплойтов**. В открывшемся окне настройте компонент в соответствии с вашими требованиями. Нажмите на кнопку **ОК**.

8. В окне **Создание групповой политики для программы** выберите одно из следующих состояний политики:

   - **Активная политика**, если требуется, чтобы политика вступила в действие сразу после ее создания. Если в группе уже существует активная политика, то она станет неактивной и будет применена новая созданная политика.

   - **Неактивная политика**, если вы не хотите сразу применять создаваемую политику. Вы сможете активировать эту политику позже.

   - Установите флажок **Открыть свойства политики сразу после создания**, чтобы автоматически закрыть **Мастер создания политики** и настроить новую политику после нажатия на кнопку **Далее**.

9. Нажмите на кнопку **Готово**.

Созданная политика отобразится в списке политик на закладке **Политики** выбранной группы администрирования. В окне **Свойства: <Имя политики>** вы можете настроить другие параметры, задачи и функции Kaspersky Embedded Systems Security.

Разделы параметров политики Kaspersky Embedded Systems Security

Общие

В разделе **Общие** вы можете настроить следующие параметры политики:

- указать состояние политики;

- настроить наследование параметров для родительских и дочерних политик.

Уведомление о событиях

В разделе **Уведомление о событиях** вы можете настроить параметры для следующих категорий событий:

- *Критическое событие*

- *Отказ функционирования*

- *Предупреждение*

- *Информационное сообщение*
  По кнопке **Свойства** вы можете настроить следующие параметры для выбранных событий:

- указать место и срок хранения информации о зарегистрированных событиях;

- выбрать способ уведомления о зарегистрированных событиях.

Параметры программы

Параметры в разделе Параметры программы

Раздел	Параметры
Масштабируемость и интерфейс	В подразделе **Масштабируемость и интерфейс** по кнопке **Настройка** вы можете настроить следующие параметры: • выбрать автоматическую или ручную настройку параметров масштабирования; • настроить параметры отображения значка программы.
Безопасность	В подразделе **Безопасность** по кнопке **Настройка** вы можете настроить следующие параметры: • настроить параметры запуска задачи; • указать действия программы при переходе защищаемого устройства на источник бесперебойного питания; • включить или выключить защиту функций программы паролем.
Параметры соединения	В подразделе **Параметры соединения** по кнопке **Настройка** вы можете настроить следующие параметры прокси-сервера для соединения с серверами обновлений, серверами активации и KSN: • указать параметры использования прокси-сервера; • указать параметры аутентификации на прокси-сервере.
Запуск системных задач	В подразделе **Запуск системных задач** по кнопке **Настройка** можно разрешить или запретить запуск следующих системных задач по расписанию, настроенному на защищаемых устройствах: • задачи проверки по требованию; • задачи обновления и копирования обновлений.

Дополнительные возможности

Параметры в разделе Дополнительные возможности

Раздел	Параметры
Доверенная зона	В подразделе **Доверенная зона** по кнопке **Настройка** вы можете настроить следующие параметры применения доверенной зоны: • сформировать список исключений доверенной зоны; • включить или выключить проверку операций резервного копирования файлов; • сформировать список доверенных процессов.
Проверка съемных	В подразделе **Проверка съемных дисков** по кнопке **Настройка** вы можете

дисков	настроить параметры проверки съемных дисков.
Права пользователей на управление программой	В подразделе **Права пользователей на управление программой** вы можете настроить параметры доступа пользователей и групп пользователей на управление Kaspersky Embedded Systems Security.
Права пользователей на управление службой Kaspersky Security	В подразделе **Права пользователей на управление службой Kaspersky Security** вы можете настроить параметры доступа пользователей и групп пользователей к управлению службой Kaspersky Security.
Хранилища	В подразделе **Хранилища** по кнопке **Настройка** вы можете настроить следующие параметры карантина, резервного хранилища и хранилища заблокированных узлов: • указать путь к папке, в которую вы хотите помещать объекты на карантине или в резервном хранилище; • настроить максимальный размер резервного хранилища и карантина, а также указать порог доступного пространства; • указать путь к папке, в которую вы хотите помещать объекты, восстановленные из резервного хранилища или карантина; • настроить продолжительность блокировки узлов.

Постоянная защита компьютера

Параметры в разделе Постоянная защита компьютера

Раздел	Параметры
Постоянная защита файлов	В подразделе **Постоянная защита файлов** по кнопке **Настройка** вы можете настроить следующие параметры задачи: • указать режим защиты объектов; • настроить применение эвристического анализатора; • настроить применение доверенной зоны; • указать область защиты; • задать уровень безопасности для выбранной области защиты: вы можете выбрать стандартный уровень безопасности или настроить параметры безопасности вручную; • настроить параметры запуска задачи.
Использование KSN	В подразделе **Использование KSN** по кнопке **Настройка** вы можете настроить следующие параметры задачи: • указать действия над объектами, недоверенными в KSN; • настроить передачу данных и использование Kaspersky Security Center в качестве прокси-сервера KSN. Нажмите на кнопку **Обработка данных**, чтобы принять или отклонить Положение о KSN и Положение о KMP, а также настроить параметры передачи данных.

Защита от эксплойтов	В подразделе **Защита от эксплойтов** по кнопке **Настройка** вы можете настроить следующие параметры задачи: • выбрать режим защиты памяти процессов; • указать действия для снижения рисков эксплуатации уязвимостей; • дополнить и изменить список защищаемых процессов.

Контроль активности на серверах

Параметры в разделе Контроль активности на компьютерах

Раздел	Параметры
Контроль запуска программ	В подразделе **Контроль запуска программ** по кнопке **Настройка** вы можете настроить следующие параметры задачи: • выбрать режим работы задачи; • настроить параметры контроля повторных запусков программ; • указать область применения правил контроля запуска программ; • настроить использование KSN; • настроить параметры запуска задачи.
Контроль устройств	В подразделе **Контроль устройств** по кнопке **Настройка** вы можете настроить следующие параметры задачи: • выбрать режим работы задачи; • настроить параметры запуска задачи.

Контроль активности в сети

Параметры в разделе Контроль активности в сети

Раздел	Параметры
Управление сетевым экраном	В подразделе **Управление сетевым экраном** по кнопке **Настройка** вы можете настроить следующие параметры задачи: • настроить правила сетевого экрана; • настроить параметры запуска задачи.

Диагностика системы

Параметры в разделе Диагностика системы

Раздел	Параметры

Мониторинг файловых операций	В подразделе **Мониторинг файловых операций** можно настроить контроль изменений в файлах, которые могут указывать на нарушение безопасности на защищаемом устройстве.
Анализ журналов	В подразделе **Анализ журналов** можно настроить контроль целостности защищаемого устройства на основе результатов анализа журнала событий Windows.

Журналы и уведомления

Параметры в разделе Журналы и уведомления

Раздел	Параметры
Журналы выполнения задач	В подразделе **Журналы выполнения задач** по кнопке **Настройка** вы можете настроить следующие параметры: • указать уровень важности регистрируемых событий для выбранных компонентов программы; • указать параметры хранения журналов выполнения задач; • указать параметры интеграции SIEM-системы с Kaspersky Security Center.
Уведомления о событиях	В подразделе **Уведомления о событиях** по кнопке **Настройка** вы можете настроить следующие параметры: • указать параметры уведомления пользователя для событий *Обнаружен объект*, *Обнаружено и запрещено недоверенное устройство* и *Компьютер добавлен в список недоверенных*; • указать параметры уведомления администратора для любого выбранного события из списка событий в разделе **Настройка уведомлений**.
Взаимодействие с Сервером администрирования	В разделе **Взаимодействие с Сервером администрирования** по кнопке **Настройка** вы можете выбрать типы объектов, включая объекты карантина и резервного хранилища, информацию о которых Kaspersky Embedded Systems Security будет передавать на Сервер администрирования.

История ревизий

В разделе **История ревизий** вы можете управлять ревизиями: сравнивать с текущей ревизией или другой политикой, добавлять описания ревизий, сохранять ревизии в файл или выполнить откат.

Настройка политики

В окне **Свойства: <Имя политики>** существующей политики можно настроить общие параметры Kaspersky Embedded Systems Security, параметры карантина и резервного хранилища, параметры доверенной зоны, параметры постоянной защиты компьютера, параметры контроля активности на компьютерах, уровень детализации в журналах выполнения задач, уведомления пользователей и администратора о событиях Kaspersky Embedded Systems Security, права доступа к управлению программой и службой Kaspersky Security.

Чтобы настроить параметры политики, выполните следующие действия:

1. В дереве Консоли администрирования Kaspersky Security Center разверните узел **Управляемые устройства**.

2. Разверните группу администрирования, параметры политики которой вы хотите настроить, и выберите в панели результатов закладку **Политики**.

3. Выберите политику, параметры которой вы хотите настроить, и откройте окно **Свойства: <Имя политики>** одним из следующих способов:

   - Выберите пункт **Свойства** в контекстном меню политики.
   - Перейдите по ссылке **Настроить параметры политики** в панели результатов выбранной политики.
   - Двойным щелчком мыши по нужной политике.

4. На закладке **Общие** в блоке **Состояние политики** включите или выключите применение политики. Для этого выберите один из следующих вариантов:

   - **Активная политика**, если вы хотите, чтобы политика применялась на всех защищаемых устройствах, входящих в выбранную группу администрирования.
   - **Неактивная политика**, если вы хотите активировать политику позже на всех защищаемых устройствах, входящих в выбранную группу администрирования.

   Вариант **Политика для автономных пользователей** недоступен при работе с Kaspersky Embedded Systems Security.

5. В разделах **Параметры событий**, **Параметры программы**, **Дополнительные возможности**, **Журналы и уведомления** и **История ревизий** можно настроить параметры программы (см. таблицу ниже).

6. В разделах **Постоянная защита компьютера**, **Контроль активности на серверах**, **Контроль активности в сети** и **Диагностика системы** можно настроить параметры программы, а также параметры запуска программы (см. таблицу ниже).

   Вы можете включать и выключать выполнение любой задачи на всех защищаемых устройствах, входящих в группу администрирования, с помощью политики Kaspersky Security Center.

   Вы можете настроить применение параметров политики на всех защищаемых устройствах сети для каждого отдельного компонента программы.

7. Нажмите на кнопку **OK**.

Настроенные параметры будут применены в политике.

Создание и настройка задач в Kaspersky Security Center

Этот раздел содержит информацию о задачах Kaspersky Embedded Systems Security, их создании, настройке параметров выполнения, запуске и остановке.

О создании задач в Kaspersky Security Center

Вы можете создавать групповые задачи для групп администрирования и для наборов защищаемых устройств. Вы можете создавать задачи следующих типов:

- Активация программы
- Копирование обновлений
- Обновление баз программы
- Обновление модулей программы
- Откат обновления баз программы
- Проверка по требованию
- Проверка целостности программы
- Мониторинг целостности файлов на основе эталона
- Формирование правил контроля запуска программ
- Формирование правил контроля устройств

Вы можете создать локальные и групповые задачи следующими способами:

- для отдельного защищаемого устройства: в окне **Свойства <Имя защищаемого устройства>** в разделе **Задачи**;
- для группы администрирования: в панели результатов узла выбранной группы защищаемых устройств на закладке **Задачи**;
- для набора защищаемых устройств: в панели результатов узла **Выборки устройств**.

С помощью политик можно отключить расписания локальных системных задач Обновление и Проверка по требованию на всех защищаемых устройствах одной группы администрирования.

Общая информация о задачах в Kaspersky Security Center приведена в *Справке Kaspersky Security Center*.

Создание задачи в Kaspersky Security Center

Чтобы создать новую задачу в Консоли администрирования Kaspersky Security Center, выполните следующие действия:

1. Запустите мастер создания задачи одним из следующих способов:
   - Для создания локальной задачи:

a. В дереве Консоли администрирования разверните узел **Управляемые устройства** и выберите группу, к которой принадлежит защищаемое устройство.

b. В панели результатов на закладке **Устройства** откройте контекстное меню защищаемого устройства и выберите пункт **Свойства**.

c. В открывшемся окне в разделе **Задачи** нажмите на кнопку **Добавить**.

- Для создания групповой задачи:

  a. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.

  b. Выберите группу администрирования, для которой требуется создать задачу.

  c. В панели результатов выберите закладку **Задачи** и выберите пункт **Создать задачу**.

- Чтобы создать задачу для произвольного набора защищаемых устройств, выполните следующие действия:

  a. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.

  b. Выберите группу администрирования, к которой принадлежат защищаемые устройства.

  c. Выберите защищаемое устройство или произвольный набор защищаемых устройств.

  d. В раскрывающемся списке **Выполнить действие** выберите **Создать задачу**.

Откроется окно мастера создания задачи.

2. В окне **Выбор типа задачи** под заголовком **Kaspersky Embedded Systems Security** выберите тип создаваемой задачи.

3. Если вы выбрали любой тип задачи, кроме Откат обновления баз программы, Проверка целостности программы и Активация программы, откроется окно **Настройка**. В зависимости от типа задачи параметры могут различаться.

   - Создайте задачу проверки по требованию.

   - Для создания задачи обновления настройте параметры задачи в соответствии с вашими требованиями:

     a. Выберите источник обновлений в окне **Источник обновлений**.

     b. Нажмите на кнопку **Настройка параметров соединения**. Откроется окно **Настройка параметров соединения**.

     c. В окне **Настройка параметров соединения** выполните следующие действия:

     Укажите режим FTP-сервера для соединения с защищаемым устройством.

     Если требуется, измените время ожидания при соединении с источником обновления.

     Настройте параметры доступа к прокси-серверу при соединении с источником обновлений.

     Укажите местоположение защищаемых устройств, чтобы оптимизировать загрузку обновлений.

- Для создания задачи Обновление модулей программы настройте параметры обновления требуемых программных модулей в окне **Настройка параметров обновления модулей программы**.

  a. Выберите либо копирование и установку критических обновлений модулей программы, либо только проверку их наличия, без установки.

  b. Если вы выбрали **Копировать и устанавливать критические обновления модулей программы**, для применения установленных программных модулей может потребоваться перезагрузка защищаемого устройства. Чтобы программа Kaspersky Embedded Systems Security автоматически запускала перезагрузку защищаемого устройства после завершения задачи, установите флажок **Разрешать перезагрузку операционной системы**.

  c. Если вы хотите получать информацию о выходе обновлений модулей Kaspersky Embedded Systems Security, установите флажок **Получать информацию о доступных плановых обновлениях модулей программы**.

  "Лаборатория Касперского" не публикует плановые пакеты обновлений на серверах обновлений для автоматической установки; вы можете загружать их с веб-сайта "Лаборатории Касперского". Можно настроить уведомление администратора о событии **Доступно плановое обновление модулей программы**. Оно будет включать адрес нашего веб-сайта, на котором можно загрузить запланированные обновления.

- Для создания задачи Копирование обновлений укажите состав обновлений и папку, в которую будут сохранены обновления, в окне **Настройка параметров копирования обновлений**.

- Для создания задачи Активация программы:

  a. В окне **Параметры активации** укажите файл ключа, с помощью которого вы хотите активировать программу.

  b. Установите флажок **Использовать в качестве дополнительного ключа**, если вы хотите создать задачу для продления срока действия лицензии.

- Создайте задачу Формирование правил контроля запуска программ.

- Создайте задачу Формирование правил контроля устройств.

4. Настройте параметры расписания задачи (вы можете настраивать расписание для всех типов задач, кроме задачи Откат обновления баз программы).

5. Нажмите на кнопку **OK**.

6. Если задача создана для набора защищаемых устройств, выберите сеть (группу) защищаемых устройств, на которых она будет выполняться.

7. В окне **Выбор учетной записи для запуска задачи** укажите учетную запись, с правами которой вы хотите выполнять задачу.

8. В окне **Определение названия задачи** введите название задачи (не более 100 символов, не должно содержать символы " * < > ? \ | :).

   Рекомендуется включить в название задачи ее тип (например, Проверка по требованию папок общего доступа).

9. В окне **Завершение создания задачи** установите флажок **Запустить задачу после завершения работы мастера**, если вы хотите, чтобы задача была запущена сразу после создания. Нажмите на кнопку **Готово**.

Созданная задача отобразится в списке **Задачи**.

Настройка локальных задач в окне Параметры программы в Kaspersky Security Center

Чтобы настроить локальные задачи или общие параметры программы для отдельного защищаемого устройства в сети, выполните следующие действия:

1. В дереве Консоли администрирования Kaspersky Security Center разверните узел **Управляемые устройства** и выберите группу, которой принадлежит защищаемое устройство.

2. В панели результатов выберите закладку **Устройства**.

3. Откройте окно **Свойства: <Имя защищаемого устройства>** одним из следующих способов:

   - двойным щелчком мыши на имени защищаемого устройства;
   - выбрав пункт **Свойства** в контекстном меню защищаемого устройства.

   Откроется окно **Свойства: <Имя защищаемого устройства>**.

4. Чтобы настроить параметры локальной задачи, выполните следующие действия:

   a. Перейдите в раздел **Задачи**.

   b. В списке задач выберите локальную задачу, параметры которой требуется настроить.

      - Откройте окно свойств задачи двойным щелчком мыши на названии задачи в списке задач.
      - Выберите название задачи и нажмите на кнопку **Свойства**.
      - Выберите пункт **Свойства** в контекстном меню выбранной задачи.

        Откроется окно **Свойства: <Название задачи>**.

5. Чтобы настроить параметры программы, выполните следующие действия:

   a. Перейдите в раздел **Программы**.

   b. В списке установленных программ выберите программу, которую требуется настроить.

      - Откройте окно параметров программы двойным щелчком мыши на названии программы в списке установленных программ.
      - Выделите название программы в списке установленных программ и нажмите на кнопку **Свойства**.
      - Откройте контекстное меню на названии программы в списке установленных программ и выберите пункт **Свойства**.

        Откроется окно **Параметры <Название программы>**.

Если программа работает под управлением политики Kaspersky Security Center и в этой политике запрещено изменять параметры программы, эти параметры недоступны для изменения в окне **Параметры <Название программы>**.

Настройка групповых задач в Kaspersky Security Center

Чтобы настроить групповую задачу для нескольких защищаемых устройств, выполните следующие действия:

1. В дереве Консоли администрирования Kaspersky Security Center разверните узел **Управляемые устройства** и выберите группу администрирования, для которой вы хотите настроить задачи.
2. В панели результатов выбранной группы администрирования выберите закладку **Задачи**.
3. В списке ранее созданных групповых задач выберите задачу, параметры которой хотите настроить. Откройте окно **Свойства: <Название задачи>** одним из следующих способов:
   - Выберите название задачи в списке созданных задач двойным щелчком мыши.
   - Выделите название задачи в списке созданных задач и перейдите по ссылке **Настроить задачу**.
   - Откройте контекстное меню задачи в списке созданных задач и выберите пункт **Свойства**.

   В разделе **Уведомления** настройте параметры уведомлений о событиях задачи. Подробная информация о настройке параметров в этом разделе приведена в *Справке Kaspersky Security Center.*
4. В зависимости от типа настраиваемой задачи выполните одно из следующих действий:
   - Если вы настраиваете задачу проверки по требованию:
     a. В разделе **Область проверки** настройте область проверки.
     b. В разделе **Параметры** настройте приоритет задачи и интеграцию с другими компонентами программы.
   - Для настройки задачи обновления укажите параметры задачи в соответствии с вашими требованиями:
     a. В разделе **Настройка** настройте параметры источника обновлений и оптимизации дисковой подсистемы.
     b. По кнопке **Настройка параметров соединения** настройте параметры соединения с источником обновлений.
   - Чтобы настроить задачу Обновление модулей программы, в разделе **Настройка параметров обновления модулей программы** выберите действие, которое требуется выполнить: копировать и устанавливать критические обновления программных модулей или только проверять их наличие.
   - Чтобы настроить задачу Копирование обновлений, в разделе **Настройка параметров копирования обновлений** укажите состав обновлений и папку назначения.
   - Если вы настраиваете задачу Активация программы, в разделе **Параметры активации** примените файл ключа, с помощью которого вы хотите активировать программу. Установите флажок **Использовать в качестве дополнительного ключа**, если вы хотите добавить код активации или файл ключа для продления срока действия лицензии.
   - Чтобы настроить задачу автоматического формирования разрешающих правил контроля устройств, в разделе **Настройка** укажите параметры, на основе которых будет сформирован список разрешающих правил.

5. В разделе **Расписание** настройте параметры расписания задачи (вы можете настраивать расписание всех задач, кроме задачи Откат обновления баз программы).

6. В разделе **Учетная запись** укажите учетную запись, с правами которой будет выполняться задача. Подробная информация о настройке параметров в этом разделе приведена в *Справке Kaspersky Security Center*.

7. Если требуется, в разделе **Исключения** из области действия задачи укажите объекты, которые хотите исключить из области действия задачи. Подробная информация о настройке параметров в этом разделе приведена в *Справке Kaspersky Security Center*.

8. В окне **Свойства: <Название задачи>** нажмите на кнопку **OK**.

Настроенные параметры групповых задач будут сохранены.

Настраиваемые параметры групповых задач приведены в следующей таблице.

Параметры групповых задач Kaspersky Embedded Systems Security

Типы задач Kaspersky Embedded Systems Security	Раздел в окне Свойства: <Название задачи>	Параметры задачи
Формирование правил контроля запуска программ	**Настройка**	При настройке параметров задачи Формирование правил контроля запуска программ вы можете выбрать способ создания разрешающих правил: • **Создавать разрешающие правила на основе запущенных программ** • **Создавать разрешающие правила для программ из папок**
	Параметры	Вы можете указать следующие действия при формировании разрешающих правил контроля запуска программ: • **Использовать цифровой сертификат** • **Использовать заголовок и отпечаток цифрового сертификата** • **Если сертификат отсутствует, использовать** • **Использовать хеш SHA256** • **Формировать правила для пользователя или группы пользователей** Вы можете настроить параметры для конфигурационных файлов со списками разрешающих правил, которые Kaspersky Embedded Systems Security создает по завершении задачи.
	Расписание	Вы можете настроить расписание запуска задачи.
Формирование правил контроля устройств	**Настройка**	• Выберите режим работы: учитывать данные системы обо всех когда-либо подключавшихся внешних устройствах или только о подключенных в настоящий момент внешних устройствах.

		• Настройте параметры для конфигурационных файлов со списками разрешающих правил, которые Kaspersky Embedded Systems Security создает по завершении задачи.
	Расписание	Вы можете настроить расписание запуска задачи.
Активация программы	**Параметры активации**	Вы можете применить файл ключа для активации программы или продления срока действия лицензии.
	Расписание	Вы можете настроить расписание запуска задачи.
Копирование обновлений	**Источник обновлений**	Вы можете указать Сервер администрирования Kaspersky Security Center или серверы обновлений "Лаборатории Касперского" в качестве источника обновлений программы. Также вы можете сформировать пользовательский список источников обновления: добавить другие HTTP-, FTP-серверы или сетевые ресурсы вручную и указать их в качестве источника обновлений. Вы можете настроить использование серверов обновлений "Лаборатории Касперского", если указанные вручную серверы недоступны.
	Окно **Параметры соединения**	В окне **Параметры соединения**, доступном из раздела **Источник обновлений**, можно указать, будет ли использоваться прокси-сервер для соединения с серверами обновлений "Лаборатории Касперского" и другими серверами.
	Настройка параметров копирования обновлений	Вы можете указать состав обновлений для копирования. В поле **Папка для локального хранения скопированных обновлений** укажите путь к папке, в которой Kaspersky Embedded Systems Security будет сохранять скопированные обновления.
	Расписание	Вы можете настроить расписание запуска задачи.
Обновление баз программы	**Настройка**	В блоке параметров **Источник обновлений** можно указать Сервер администрирования Kaspersky Security Center или серверы обновлений "Лаборатории Касперского" в качестве источника обновлений программы. Также вы можете сформировать пользовательский список источников обновления: добавить другие HTTP-, FTP-серверы или сетевые ресурсы вручную и указать их в качестве источника обновлений. Вы можете настроить использование серверов обновлений "Лаборатории Касперского", если указанные вручную серверы недоступны. В блоке Оптимизация использования дисковой подсистемы вы можете настроить параметры функции, снижающей нагрузку на дисковую подсистему: • **Снизить нагрузку на дисковую подсистему** • **Объем оперативной памяти, используемый для оптимизации (МБ)**
	Окно **Параметры соединения**	В окне **Параметры соединения**, доступном из раздела **Источник обновлений**, можно указать, будет ли использоваться прокси-сервер для соединения с серверами обновлений "Лаборатории Касперского" и другими серверами.
	Расписание	Вы можете настроить расписание запуска задачи.
Обновление	**Источник**	Вы можете указать Сервер администрирования Kaspersky Security

модулей программы	**обновлений**	Center или серверы обновлений "Лаборатории Касперского" в качестве источника обновлений программы. Также вы можете сформировать пользовательский список источников обновления: добавить другие HTTP-, FTP-серверы или сетевые ресурсы вручную и указать их в качестве источника обновлений. Вы можете настроить использование серверов обновлений "Лаборатории Касперского", если указанные вручную серверы недоступны.
	Окно **Параметры соединения**	В блоке параметров **Параметры соединения с источниками обновлений** можно указать, будет ли использоваться прокси-сервер для соединения с серверами обновлений "Лаборатории Касперского" и другими серверами.
	Настройка параметров обновления модулей программы	Вы можете указать действия, которые Kaspersky Embedded Systems Security будет совершать при наличии критических обновлений модулей программы, а также по завершении установки критических обновлений. Кроме того, можно указать, будет ли Kaspersky Embedded Systems Security получать информацию о доступных плановых обновлениях.
	Расписание	Вы можете настроить расписание запуска задачи.
Параметры проверки по требованию	**Область проверки**	Вы можете сформировать область проверки для задачи проверки по требованию и настроить параметры уровня безопасности.
	Окно **Настройка проверки по требованию**	В окне **Настройка проверки по требованию**, доступном из раздела **Область проверки**, вы можете выбрать один из стандартных уровней безопасности или настроить уровень безопасности вручную.
	Параметры	В блоке параметров **Эвристический анализатор** вы можете включить или выключить применение эвристического анализатора в задаче проверки по требованию и настроить уровень анализа с помощью ползунка. В блоке **Дополнительные параметры** можно настроить следующие параметры: • применение Доверенной зоны в задачах проверки по требованию; • применение служб KSN в задачах проверки по требованию; • указать приоритет задачи проверки по требованию: выполнять задачу в фоновом режиме (низкий приоритет) или считать выполнение задачи проверкой важных областей.
	Расписание	Вы можете настроить расписание запуска задачи.
Проверка целостности программы	**Расписание**	Вы можете настроить расписание запуска задачи.
Мониторинг целостности файлов на основе эталона	**Расписание**	Вы можете настроить расписание запуска задачи.

Для задачи Откат обновления баз программы можно настроить только стандартные параметры задачи, регулируемые Kaspersky Security Center, в разделах **Уведомления** и **Исключения из области действия задачи**.

Подробная информация о настройке параметров в этом разделе приведена в *Справке Kaspersky Security Center*.

Задача Активация программы

Чтобы настроить задачу Активация программы, выполните следующие действия:

1. В дереве Консоли администрирования Kaspersky Security Center разверните узел **Управляемые устройства** и выберите группу администрирования, для которой вы хотите настроить задачи.
2. В панели результатов выбранной группы администрирования выберите закладку **Задачи**.
3. В списке ранее созданных групповых задач выберите задачу, параметры которой хотите настроить. Откройте окно **Свойства: <Название задачи>** одним из следующих способов:
   - Выберите название задачи в списке созданных задач двойным щелчком мыши.
   - Выделите название задачи в списке созданных задач и перейдите по ссылке **Настроить задачу**.
   - Откройте контекстное меню задачи в списке созданных задач и выберите пункт **Свойства**.

   В разделе **Уведомления** настройте параметры уведомлений о событиях задачи. Подробная информация о настройке параметров в этом разделе приведена в *Справке Kaspersky Security Center.*
4. В разделе **Параметры активации** укажите файл ключа, с помощью которого вы хотите активировать программу. Установите флажок **Использовать в качестве дополнительного ключа**, если вы хотите добавить ключ для продления срока действия лицензии.
5. В разделе **Расписание** настройте параметры расписания задачи (вы можете настраивать расписание всех задач, кроме задачи Откат обновления баз программы).
6. В разделе **Учетная запись** укажите учетную запись, с правами которой будет выполняться задача.
7. Если требуется, в разделе **Исключения** из области действия задачи укажите объекты, которые хотите исключить из области действия задачи.

   Подробная информация о настройке параметров в этом разделе приведена в *Справке Kaspersky Security Center*.
8. В окне **Свойства: <Название задачи>** нажмите на кнопку **OK**.

   Настроенные параметры групповых задач будут сохранены.

Задачи обновления

Чтобы настроить задачи Копирование обновлений, Обновление баз программы или Обновление модулей программы, выполните следующие действия:

1. В дереве Консоли администрирования Kaspersky Security Center разверните узел **Управляемые устройства** и выберите группу администрирования, для которой вы хотите настроить задачи.

2. В панели результатов выбранной группы администрирования выберите закладку **Задачи**.

3. В списке ранее созданных групповых задач выберите задачу, параметры которой хотите настроить. Откройте окно **Свойства: <Название задачи>** одним из следующих способов:

   - Выберите название задачи в списке созданных задач двойным щелчком мыши.
   - Выделите название задачи в списке созданных задач и перейдите по ссылке **Настроить задачу**.
   - Откройте контекстное меню задачи в списке созданных задач и выберите пункт **Свойства**.

   В разделе **Уведомления** настройте параметры уведомлений о событиях задачи. Подробная информация о настройке параметров в этом разделе приведена в *Справке Kaspersky Security Center.*

4. В зависимости от типа настраиваемой задачи выполните одно из следующих действий:

   - В разделе **Источник обновлений** настройте параметры источника обновлений и оптимизации дисковой подсистемы.

     a. В разделе **Источник обновлений** вы можете указать Сервер администрирования Kaspersky Security Center или серверы обновлений "Лаборатории Касперского" в качестве источника обновлений программы. Также вы можете сформировать пользовательский список источников обновления: добавить другие HTTP-, FTP-серверы или сетевые ресурсы вручную и указать их в качестве источника обновлений.

     Вы можете настроить использование серверов обновлений "Лаборатории Касперского", если указанные вручную серверы недоступны.

     Чтобы использовать в качестве источника обновлений общую папку SMB, необходимо указать учетную запись, с правами которой запускается задача.

     b. В разделе **Оптимизация использования дисковой подсистемы** для задачи Обновление баз программы вы можете настроить следующие параметры функции, снижающей нагрузку на дисковую подсистему:

     - **Снизить нагрузку на дисковую подсистему**
     - **Объем оперативной памяти, используемый для оптимизации (МБ)**

     c. Нажмите на кнопку **Настройка параметров соединения** и в открывшемся окне **Настройка параметров соединения** настройте параметры использования прокси-сервера для соединения с серверами обновлений "Лаборатории Касперского" и другими серверами.

- В разделе **Настройка параметров обновления модулей программы** для задачи Обновление модулей программы вы можете указать действия, которые Kaspersky Embedded Systems Security будет совершать при наличии критических обновлений модулей программы или при наличии информации о плановых обновлениях, а также настроить действия программы по завершении установки критических обновлений.

- В разделе **Настройка параметров копирования обновлений** укажите состав обновлений и папку, в которую будут сохранены обновления, для задачи Копирование обновлений.

5. В разделе **Расписание** настройте параметры расписания задачи (вы можете настраивать расписание всех задач, кроме задачи Откат обновления баз программы).

6. В разделе **Учетная запись** укажите учетную запись, с правами которой будет выполняться задача.

   Подробная информация о настройке параметров в этом разделе приведена в *Справке Kaspersky Security Center*.

7. В окне **Свойства: <Название задачи>** нажмите на кнопку **ОК**.

Настроенные параметры групповых задач будут сохранены.

Для задачи Откат обновления баз программы можно настроить только стандартные параметры задачи, контролируемые Kaspersky Security Center, в разделах **Уведомления** и **Исключения из области действия задачи**. Подробная информация о настройке параметров в этом разделе приведена в *Справке Kaspersky Security Center*.

Проверка целостности программы

Чтобы настроить групповую задачу Проверка целостности программы, выполните следующие действия:

1. В дереве Консоли администрирования Kaspersky Security Center разверните узел **Управляемые устройства** и выберите группу администрирования, для которой вы хотите настроить задачи.

2. В панели результатов выбранной группы администрирования выберите закладку **Задачи**.

3. В списке ранее созданных групповых задач выберите задачу, параметры которой хотите настроить. Откройте окно **Свойства: <Название задачи>** одним из следующих способов:

   - Выберите название задачи в списке созданных задач двойным щелчком мыши.

   - Выделите название задачи в списке созданных задач и перейдите по ссылке **Настроить задачу**.

   - Откройте контекстное меню задачи в списке созданных задач и выберите пункт **Свойства**.

   В разделе **Уведомления** настройте параметры уведомлений о событиях задачи. Подробная информация о настройке параметров в этом разделе приведена в *Справке Kaspersky Security Center.*

4. В разделе **Устройства** выберите устройства, для которых требуется настроить задачу Проверка целостности программы.

5. В разделе **Расписание** настройте параметры расписания задачи (вы можете настраивать расписание всех задач, кроме задачи Откат обновления баз программы).

6. В разделе **Учетная запись** укажите учетную запись, с правами которой будет выполняться задача.

7. Если требуется, в разделе **Исключения** из области действия задачи укажите объекты, которые хотите исключить из области действия задачи.

   Подробная информация о настройке параметров в этом разделе приведена в *Справке Kaspersky Security Center*.

8. В окне **Свойства: <Название задачи>** нажмите на кнопку **OK**.

   Настроенные параметры групповых задач будут сохранены.

Настройка параметров диагностики сбоев в Kaspersky Security Center

Если в работе Kaspersky Embedded Systems Security возникла проблема (например, аварийное завершение Kaspersky Embedded Systems Security) и вы хотите диагностировать ее, вы можете включить создание файлов трассировки и файла дампа процессов Kaspersky Embedded Systems Security и отправить эти файлы на анализ в Службу технической поддержки "Лаборатории Касперского".

Kaspersky Embedded Systems Security не отправляет файлы трассировки и файлы дампов автоматически. Диагностические данные могут быть отправлены только пользователем с соответствующими правами.

Kaspersky Embedded Systems Security записывает информацию в файлы трассировки и файлы дампов в незашифрованном виде. Папка, в которую сохраняются файлы, выбирается пользователем и контролируется параметрами операционной системы и Kaspersky Embedded Systems Security. Можно настроить права доступа и разрешить доступ к журналам, файлам трассировки и файлам дампов только для выбранных пользователей.

Чтобы настроить параметры диагностики сбоев в Kaspersky Security Center, выполните следующие действия:

1. В Консоли администрирования Kaspersky Security Center откройте окно **Параметры программы**.

2. Откройте раздел **Диагностика сбоев** и выполните следующие действия:

   - Если вы хотите записывать отладочную информацию в файл, установите флажок **Записывать отладочную информацию в файл трассировки**.
     - В поле ниже укажите папку, в которую Kaspersky Embedded Systems Security будет сохранять файлы трассировки.
     - Настройте уровень детализации отладочной информации.
     - Укажите максимальный размер файлов трассировки.
     - Укажите максимальное количество файлов в одном журнале трассировки.

Kaspersky Embedded Systems Security создает не более указанного максимального количества файлов трассировки для каждого отлаживаемого компонента.

- Укажите отлаживаемые компоненты. Коды компонентов требуется вводить через запятую и с соблюдением регистра (см. таблицу ниже).

Коды подсистем Kaspersky Embedded Systems Security

Код подсистемы	Название подсистемы
*	Все компоненты.
gui	Подсистема пользовательского интерфейса, оснастка Kaspersky Embedded Systems Security в Microsoft Management Console.
ak_conn	Подсистема интеграции с Агентом администрирования Kaspersky Security Center.
bl	Управляющий процесс, реализует задачи управления Kaspersky Embedded Systems Security.
wp	Рабочий процесс; реализует задачи антивирусной защиты.
blgate	Процесс удаленного управления Kaspersky Embedded Systems Security.
ods	Подсистема проверки по требованию.
oas	Подсистема постоянной защиты файлов.
qb	Подсистема карантина и резервного хранилища.
scandll	Вспомогательный модуль антивирусной проверки.
core	Подсистема базовой антивирусной функциональности.
avscan	Подсистема антивирусной обработки.
avserv	Подсистема управления антивирусным ядром.
prague	Подсистема базовой функциональности.
updater	Подсистема обновления баз и модулей программы.
snmp	Подсистема поддержки SNMP протокола.
perfcount	Подсистема счетчиков производительности.

Параметры трассировки оснастки Kaspersky Embedded Systems Security (gui) и Плагина управления для Kaspersky Security Center (ak_conn) применяются после перезапуска этих компонентов. Параметры трассировки подсистемы поддержки SNMP-протокола (snmp) применяются после перезапуска службы SNMP. Параметры трассировки подсистемы счетчиков производительности (perfcount) применяются после перезапуска всех процессов, использующих счетчики производительности. Параметры трассировки остальных подсистем Kaspersky Embedded Systems Security применяются сразу после сохранения параметров диагностики сбоев.

По умолчанию Kaspersky Embedded Systems Security сохраняет отладочную информацию о работе всех компонентов Kaspersky Embedded Systems Security.

Поле ввода доступно, если установлен флажок **Записывать отладочную информацию в файл трассировки**.

- Если вы хотите, чтобы создавался файл дампа, установите флажок **Создавать во время сбоя файл дампа**.

  - В поле ниже укажите папку, в которую Kaspersky Embedded Systems Security будет сохранять файл дампа.

3. Нажмите на кнопку **OK**.

Настроенные параметры программы будут применены на защищаемом устройстве.

Работа с расписанием задач

Можно настроить расписание запуска задач Kaspersky Embedded Systems Security, а также настроить параметры запуска по расписанию.

Настройка расписания запуска задач

В Консоли программы вы можете настроить расписание запуска локальных системных и пользовательских задач. Расписание запуска групповых задач настраивать нельзя.

Чтобы настроить расписание запуска групповой задачи, выполните следующие действия:

1. В дереве Консоли администрирования Kaspersky Security Center разверните узел **Управляемые устройства**.
2. Выберите группу, к которой принадлежит защищаемое устройство.
3. В панели результатов выберите закладку **Задачи**.
4. Откройте окно **Свойства: <Название задачи>** одним из следующих способов:
   - двойным щелчком мыши по имени задачи;
   - выбрав пункт Свойства в контекстном меню задачи.
5. Выберите раздел **Расписание**.
6. В блоке **Параметры расписания** установите флажок **Запускать задачу по расписанию**.

   Поля с параметрами расписания задачи проверки по требованию и задачи обновления недоступны, если запуск этих задач по расписанию запрещен политикой Kaspersky Security Center.

7. Настройте параметры расписания в соответствии с вашими требованиями. Для этого выполните следующие действия:

   a. в списке **Частота запуска** выберите одно из следующих значений:

   - **Ежечасно**, если вы хотите, чтобы задача запускалась периодически через заданное количество часов, и укажите количество часов в поле **Раз в <количество> часов**.
   - **Ежесуточно**, если вы хотите, чтобы задача запускалась периодически через заданное количество дней, и укажите количество дней в поле **Раз в <количество> дней**.
   - **Еженедельно**, если вы хотите, чтобы задача запускалась периодически через заданное количество недель, и укажите количество недель в поле **Раз в <количество> недель**. Укажите, по каким дням недели будет запускаться задача (по умолчанию задача запускается по понедельникам).

- **При запуске программы**, если вы хотите, чтобы задача запускалась при каждом запуске Kaspersky Embedded Systems Security.
- **После обновления баз программы**, если вы хотите, чтобы задача запускалась после каждого обновления баз программы.

b. В поле **Время запуска** укажите время первого запуска задачи.

c. В поле **Начать с** укажите дату начала действия расписания.

После того как вы укажете частоту и время первого запуска задачи и дату начала действия расписания, в верхней части окна в поле **Следующий запуск** отобразится расчетное время очередного запуска задачи. Расчетное время следующего запуска задачи будет обновляться каждый раз, когда вы открываете окно **Параметры задачи** на закладке **Расписание**.

Значение **Запрещен политикой** отображается в поле **Следующий запуск**, если параметрами действующей политики Kaspersky Security Center запрещен запуск системных задач по расписанию.

8. На закладке **Дополнительно** настройте следующие параметры расписания в соответствии с вашими требованиями.
   - В блоке **Параметры остановки задачи**:
     a. Установите флажок **Длительность** и в полях справа укажите максимальную длительность выполнения задачи (количество часов и минут).
     b. Установите флажок **Приостановить с** и в полях справа укажите начальное и конечное значение временного промежутка в пределах суток, в течение которого выполнение задачи будет приостановлено.
   - В блоке **Дополнительные параметры**:
     a. Установите флажок **Отменить расписание с** и укажите дату, начиная с которой расписание перестанет действовать.
     b. Установите флажок **Запускать пропущенные задачи**, чтобы включить запуск пропущенных задач.
     c. Установите флажок **Распределять время запуска задач в интервале** и укажите значение параметра в минутах.
9. Нажмите на кнопку **OK**.
10. Нажмите на кнопку **Применить**, чтобы сохранить параметры запуска задачи.

Если вы хотите настроить параметры программы для отдельной задачи с помощью Kaspersky Security Center, выполните действия, описанные в разделе "Настройка локальных задач в окне Параметры программы в Kaspersky Security Center".

Включение и выключение запуска задач по расписанию

Вы можете включать и выключать запуск задач по расписанию как после, так и до настройки параметров расписания.

Чтобы включить или выключить расписание запуска задачи, выполните следующие действия:

1. В дереве Консоли администрирования Kaspersky Security Center разверните узел **Управляемые устройства**.
2. Выберите группу, к которой принадлежит защищаемое устройство.
3. В панели результатов выберите закладку **Задачи**.
4. Откройте окно **Свойства: <Название задачи>** одним из следующих способов:
   - двойным щелчком мыши по имени задачи;
   - выбрав пункт Свойства в контекстном меню задачи.
5. Выберите раздел **Расписание**.
6. Выполните одно из следующих действий:
   - Установите флажок **Запускать задачу по расписанию**, если вы хотите включить запуск задачи по расписанию.
   - Снимите флажок **Запускать задачу по расписанию**, если вы хотите выключить запуск задачи по расписанию.

     Настроенные параметры расписания запуска задачи не будут удалены и применятся при следующем включении запуска задачи по расписанию.
7. Нажмите на кнопку **OK**.
8. Нажмите на кнопку **Применить**.

Настроенные параметры запуска задачи по расписанию будут сохранены.

Отчеты в Kaspersky Security Center

Отчеты в Kaspersky Security Center содержат информацию о состоянии управляемых устройств. Отчеты формируются на основании информации, хранящейся на Сервере администрирования.

Начиная с Kaspersky Security Center 11, для Kaspersky Embedded Systems Security доступны следующие типы отчетов:

- отчет о статусе компонентов;
- отчет о запрещенных запусках;

- отчет о тестовых запрещенных запусках.

Подробную информацию о настройке и работе с отчетами Kaspersky Security Center см. в *Справке Kaspersky Security Center*.

Отчет о статусе компонентов Kaspersky Embedded Systems Security

Вы можете контролировать состояние защиты всех устройств в сети и получать организованное представление о наборе компонентов на каждом устройстве.

В отчете для каждого компонента может отображаться одно из следующих состояний: *Работает*, *Приостановлен*, *Остановлен*, *Неисправен*, *Не установлен*, *Запускается*.

Состояние *Не установлен* относится к компонентам программы, а не к самой программе. Если программа не установлена, Kaspersky Security Center присваивает статус N/A (недоступно).

Можно создавать выборки компонентов и использовать фильтры, чтобы отображать сетевые устройства с определенным набором компонентов и их состояниями.

Подробную информацию о создании и использовании выборок см. в *Справке Kaspersky Security Center*.

Чтобы просмотреть статусы компонентов в параметрах программы, выполните следующие действия:

1. В дереве Консоли администрирования Kaspersky Security Center разверните узел **Управляемые устройства** и выберите группу администрирования, для которой вы хотите настроить параметры программы.
2. Выберите закладку **Устройства** и откройте окно **Параметры программы**.
3. Выберите раздел **Компоненты**.
4. Ознакомьтесь с таблицей состояния компонентов.

Чтобы просмотреть стандартный отчет Kaspersky Security Center, выполните следующие действия:

1. В дереве Консоли администрирования выберите узел **Сервер администрирования <Имя Сервера администрирования>**.
2. Выберите закладку **Отчеты**.
3. Откройте **Отчет о статусе компонентов программы** двойным щелчком мыши.

   Будет сформирован отчет.
4. Ознакомьтесь со следующими элементами отчета:
   - диаграмма;
   - итоговая таблица с компонентами и суммарным количеством устройств в сети, на которых установлен каждый из компонентов, а также группы, к которым они принадлежат;

- детальная таблица, показывающая статус, версию, устройство и группу компонента.

Отчеты о запрещенных программах в активном и в тестовом режимах

По результатам выполнения задачи Контроль запуска программ можно сформировать два типа отчетов: отчет о запрещенных программах (если задача запущена в активном режиме) и отчет о запрещенных программах в тестовом режиме (если задача запущена в режиме Только статистика). В этих отчетах приведена информация о заблокированных программах на защищаемых устройствах сети. Каждый отчет формируется для всех групп администрирования и содержит данные обо всех программах "Лаборатории Касперского", установленных на защищаемых устройствах.

Чтобы просмотреть отчет о запрещенных программах в режиме Только статистика, выполните следующие действия:

1. Запустите задачу Контроль запуска программ в режиме Только статистика.
2. В дереве Консоли администрирования выберите узел **Сервер администрирования <Имя Сервера администрирования>**.
3. Выберите закладку **Отчеты**.
4. Откройте **Отчет о запрещенных программах в режиме тестирования** двойным щелчком мыши.

   Будет сформирован отчет.
5. Ознакомьтесь со следующими элементами отчета:

   - диаграмма, показывающая десять программ с самым большим количеством заблокированных запусков;
   - итоговая таблица блокировок программ, содержащая имя исполняемого файла, причину и время блокировки, а также количество устройств, на которых произошла блокировка программ;
   - детальная таблица, показывающая данные устройства, путь к файлу и причину блокировки.

Чтобы просмотреть отчет о запрещенных программах в активном режиме, выполните следующие действия:

1. Запустите задачу Контроль запуска программ в режиме Активный.
2. В дереве Консоли администрирования выберите узел **Сервер администрирования <Имя Сервера администрирования>**.
3. Выберите закладку **Отчеты**.
4. Откройте **Отчет о запрещенных программах** двойным щелчком мыши.

   Будет сформирован отчет.

Отчет содержит те же разделы данных, что и отчет о запрещенных программах в тестовом режиме.

Работа с Консолью Kaspersky Embedded Systems Security

Этот раздел содержит информацию о Консоли Kaspersky Embedded Systems Security и об управлении программой через Консоль программы, установленную на защищаемом устройстве или другом устройстве.

О Консоли Kaspersky Embedded Systems Security

Консоль Kaspersky Embedded Systems Security представляет собой изолированную оснастку, которая добавляется в Microsoft Management Console.

Вы можете управлять программой через Консоль программы, установленную на защищаемом устройстве или на другом устройстве в сети организации.

После установки Консоли программы на другое устройство требуется дополнительная настройка.

Если Консоль программы и Kaspersky Embedded Systems Security установлены на разных защищаемых устройствах, принадлежащих к разным доменам, возможны ограничения в передаче информации от Kaspersky Embedded Systems Security на Консоль программы. Например, после запуска какой-либо задачи статус этой задачи может не обновиться в Консоли программы.

При установке Консоли программы в папке установки создается файл kavfs.msc, а оснастка Kaspersky Embedded Systems Security добавляется в список изолированных оснасток Microsoft Windows.

Вы можете запустить Консоль программы из меню **Пуск**. Вы можете запустить msc-файл оснастки Kaspersky Embedded Systems Security или добавить оснастку программы в Microsoft Management Console как новый элемент в дереве.

В 64-разрядной версии Microsoft Windows вы можете добавить оснастку Kaspersky Embedded Systems Security только в Microsoft Management Console 32-разрядной версии. Для этого откройте Microsoft Management Console из командной строки с помощью команды mmc.exe /32.

Можно добавить несколько оснасток Kaspersky Embedded Systems Security в Microsoft Management Console в авторском режиме, чтобы управлять защитой нескольких устройств, на которых установлена программа Kaspersky Embedded Systems Security.

Интерфейс Консоли Kaspersky Embedded Systems Security

В этом разделе описаны основные элементы интерфейса программы.

Окно консоли Kaspersky Embedded Systems Security

Консоль Kaspersky Embedded Systems Security отображается в дереве Microsoft Management Console в виде узла.

После подключения к программе Kaspersky Embedded Systems Security, установленной на другом защищаемом устройстве, в название узла добавляется имя защищаемого устройства, на котором установлена программа, и имя учетной записи, с правами которой выполнено подключение: **Kaspersky Embedded Systems Security <имя защищаемого устройства> как <имя учетной записи>**. При подключении к программе Kaspersky Embedded Systems Security, установленной на том же защищаемом устройстве, что и Консоль программы, узел называется **Kaspersky Embedded Systems Security**.

Дерево Консоли программы

В дереве Консоли программы отображается узел **Kaspersky Embedded Systems Security** и вложенные узлы функциональных компонентов программы.

Узел **Kaspersky Embedded Systems Security** содержит следующие вложенные узлы:

- **Постоянная защита компьютера**: управление задачами постоянной защиты компьютеров и службами KSN. Узел **Постоянная защита компьютера** позволяет управлять следующими задачами:
  - **Постоянная защита файлов**
  - **Использование KSN**
- **Контроль компьютера**: контроль программ, запускаемых на защищаемом устройстве, и подключаемых устройств. Узел **Контроль компьютера** позволяет настраивать следующие задачи:
  - **Контроль запуска программ**
  - **Контроль устройств**
  - **Управление сетевым экраном**
- **Автоматическое формирование правил**: настройка автоматического формирования групповых и системных правил для задач Контроль запуска программ и Контроль устройств.
  - **Формирование правил контроля запуска программ**
  - **Формирование правил контроля устройств**
  - Групповые задачи формирования правил **<Имена задач>** (если есть)

    Групповые задачи создаются с помощью Kaspersky Security Center. Вы не можете управлять групповыми задачами через Консоль программы.
- **Диагностика системы**: настройка параметров контроля файловых операций и анализа журнала событий Windows.
  - **Мониторинг файловых операций**
  - **Анализ журналов**
- **Проверка по требованию**: управление задачами проверки по требованию. Для каждой задачи предусмотрен свой элемент управления:
  - **Проверка при старте операционной системы**
  - **Проверка важных областей**

- **Проверка объектов на карантине**
- **Проверка целостности программы**
- Пользовательские задачи **<Имена задач>** (если есть)

В узле отображаются системные задачи, созданные при установке программы, пользовательские задачи и групповые задачи проверки по требованию, сформированные и переданные на защищаемое устройство с помощью Kaspersky Security Center.

- **Обновление**: управление обновлением баз и модулей Kaspersky Embedded Systems Security, а также копированием обновлений в папку локального источника обновлений. Узел содержит вложенные узлы для управления всеми задачами обновления, а также последней задачей **Откат обновления баз программы**:
  - **Обновление баз программы**
  - **Обновление модулей программы**
  - **Копирование обновлений**
  - **Откат обновления баз программы**

  В узле отображаются все пользовательские и групповые задачи обновлений, сформированные и переданные на защищаемое устройство с помощью Kaspersky Security Center.

- **Хранилища**: управление параметрами карантина и резервного хранилища.
  - **Карантин**
  - **Резервное хранилище**

- **Журналы и уведомления**: управление журналами выполнения локальных задач, журналом безопасности и журналом системного аудита Kaspersky Embedded Systems Security.
  - **Журнал событий безопасности**
  - **Журнал системного аудита**
  - **Журналы выполнения задач**

- **Лицензирование**: добавление и удаление ключей Kaspersky Embedded Systems Security, просмотр информации о лицензиях.

Панель результатов

В панели результатов отображается информация о выбранном узле. Если выбран узел **Kaspersky Embedded Systems Security**, в панели результатов отобразится информация о текущем состоянии защиты устройства, информация о Kaspersky Embedded Systems Security, состояние защиты функциональных компонентов программы и дата истечения срока действия лицензии.

Контекстное меню узла Kaspersky Embedded Systems Security

С помощью пунктов контекстного меню узла **Kaspersky Embedded Systems Security** можно выполнять следующие операции:

- **Подключиться к другому компьютеру**. Подключиться к другому устройству, чтобы управлять установленной на нем программой Kaspersky Embedded Systems Security. Для выполнения этой операции вы можете также воспользоваться ссылкой в правом нижнем углу панели результатов узла **Kaspersky Embedded Systems Security**.

- **Запустить программу** / **Остановить программу**. Запустить или остановить программу или выбранную задачу. Для выполнения этих операций вы также можете воспользоваться кнопками в панели инструментов. Выполнение этих операций также доступно в контекстных меню задач программы.

- **Настроить проверку съемных дисков**. Настроить проверку съемных дисков, подключенных к защищаемому устройству по USB.

- **Защита от эксплойтов: общие параметры защиты**. Настроить режим защиты от эксплойтов и профилактические действия.

- **Защита от эксплойтов: параметры защиты процессов**. Добавить процессы, которые нужно защитить, и выбрать техники защиты от эксплойтов.

- **Настроить параметры доверенной зоны**. Просмотреть и настроить параметры доверенной зоны.

- **Изменить права пользователей на управление программой**. Просмотреть и настроить права доступа к функциям Kaspersky Embedded Systems Security.

- **Изменить права пользователей на управление службой Kaspersky Security**. Просмотреть и настроить права пользователя на управление службой Kaspersky Security.

- **Экспортировать параметры**. Сохранить параметры программы в конфигурационный файл в формате XML. Выполнение этой операции также доступно в контекстных меню задач программы.

- **Импортировать параметры**. Импортировать параметры программы из конфигурационного файла в формате XML. Выполнение этой операции также доступно в контекстных меню задач программы.

- **Данные о программе и доступных обновлениях**. Перейти к просмотру информации о Kaspersky Embedded Systems Security и текущих доступных обновлениях модулей программы.

- **Обновить**. Обновить содержимое окна Консоли программы. Выполнение этой операции также доступно в контекстных меню задач программы.

- **Свойства**. Просмотреть и настроить параметры работы Kaspersky Embedded Systems Security или выбранной задачи. Выполнение этой операции также доступно в контекстных меню задач программы.

  Для выполнения этой операции вы также можете воспользоваться ссылкой **Свойства программы** в панели результатов узла **Kaspersky Embedded Systems Security** или кнопкой на панели инструментов.

- **Справка**. Перейти к просмотру справочной системы Kaspersky Embedded Systems Security. Выполнение этой операции также доступно в контекстных меню задач программы.

Панель инструментов и контекстное меню задач Kaspersky Embedded Systems Security

Вы можете управлять задачами Kaspersky Embedded Systems Security с помощью пунктов контекстного меню каждой задачи в дереве Консоли программы.

С помощью пунктов контекстного меню выбранной задачи вы можете выполнять следующие операции:

- **Запустить** / **Остановить**. Запустить или остановить выполнение задачи. Для выполнения этих операций вы также можете воспользоваться кнопками в панели инструментов.
- **Возобновить** / **Приостановить**. Возобновить или приостановить выполнение задачи. Для выполнения этих операций вы также можете воспользоваться кнопками в панели инструментов. Операция доступна для задач постоянной защиты компьютера и задач проверки по требованию.
- **Добавить задачу**. Создать новую пользовательскую задачу. Операция доступна для задач проверки по требованию.
- **Открыть журнал выполнения**. Просматривать журнал выполнения задачи и управлять им. Операция доступна для всех задач.
- **Удалить задачу**. Удалить пользовательскую задачу. Операция доступна для задач проверки по требованию.
- **Шаблоны параметров**. Управлять шаблонами. Операция доступна для задачи Постоянная защита файлов и задач проверки по требованию.

Значок области уведомлений в панели задач

Каждый раз, когда Kaspersky Embedded Systems Security автоматически запускается после перезагрузки защищаемого устройства, в области уведомлений панели задач отображается значок области уведомлений . Он отображается по умолчанию, если при установке программы вы установили компонент Значок области уведомлений.

Вид значка области уведомлений отражает текущий статус защиты устройства. Возможны следующие два статуса:

	активный (цветной значок), если выполняется хотя бы одна из задач: Постоянная защита файлов, Контроль запуска программ;
	неактивный (серый значок), если не выполняется ни одна из задач: Постоянная защита файлов, Контроль запуска программ.

Вы можете открыть контекстное меню значка области уведомлений по правой клавише мыши.

Контекстное меню включает несколько команд, предназначенных для отображения окон программы (см. таблицу ниже).

Команды контекстного меню, отображаемые с помощью значка области уведомлений

Команда	Описание
Открыть Консоль управления	Открывает Консоль Kaspersky Embedded Systems Security (если она установлена).
Открыть Диагностическое окно	Открывает Диагностическое окно программы.
О программе	Открывает окно О программе с информацией о Kaspersky Embedded Systems Security. Если вы зарегистрированы в качестве пользователя Kaspersky Embedded Systems Security, окно О программе содержит информацию об установленных срочных обновлениях.

Скрыть	Скрывает значок области уведомлений в панели задач.

Скрытый значок области уведомлений можно отобразить в любое время.

Чтобы снова отобразить значок области уведомлений,

в Microsoft Windows в меню **Пуск** выберите **Все программы** > **Kaspersky Embedded Systems Security** > **Значок области уведомлений**.

Названия параметров могут отличаться в зависимости от версии установленной операционной системы.

В общих параметрах Kaspersky Embedded Systems Security можно включать и выключать отображение значка области уведомлений при автоматическом запуске программы после перезагрузки защищаемого устройства.

Управление Kaspersky Embedded Systems Security через Консоль программы, установленную на другом устройстве

Вы можете управлять Kaspersky Embedded Systems Security через Консоль программы, которая установлена на удаленном устройстве.

Чтобы управление программой с помощью Консоли Kaspersky Embedded Systems Security, установленной на удаленном устройстве, было доступно, убедитесь, что выполняются следующие условия:

- Пользователи Консоли программы на удаленном устройстве добавлены в группу ESS Administrators на защищаемом устройстве.
- Разрешены сетевые соединения для процесса службы Kaspersky Security Management (kavfsgt.exe), если на защищаемом устройстве включен брандмауэр Windows.
- Во время установки Kaspersky Embedded Systems Security в окне мастера установки был установлен флажок **Разрешить удаленный доступ**.

Если программа Kaspersky Embedded Systems Security на удаленном устройстве защищена паролем, введите пароль для получения доступа к управлению программой через Консоль программы.

Настройка общих параметров программы в Консоли программы

Общие параметры и параметры диагностики сбоев Kaspersky Embedded Systems Security определяют общие условия работы программы. Эти параметры позволяют контролировать количество рабочих процессов, используемых Kaspersky Embedded Systems Security, включать восстановление задач Kaspersky Embedded Systems Security после их аварийного завершения, вести журнал, включать создание файлов дампов для процессов Kaspersky Embedded Systems Security при их аварийном завершении и настраивать другие общие параметры.

Настройка параметров программы недоступна из Консоли программы, если изменение данных параметров запрещено активной политикой Kaspersky Security Center.

Чтобы настроить параметры Kaspersky Embedded Systems Security, выполните следующие действия:

1. В дереве Консоли программы выберите узел **Kaspersky Embedded Systems Security** и выполните одно из следующих действий:

   - В панели результатов узла перейдите по ссылке **Свойства программы**.
   - В контекстном меню узла выберите пункт **Свойства**.

   Откроется окно **Параметры программы**.

2. В открывшемся окне настройте общие параметры Kaspersky Embedded Systems Security согласно вашим требованиям:

   - На закладке **Масштабируемость и интерфейс** можно настроить следующие параметры:
     - В разделе **Параметры масштабируемости**:
       - Максимальное количество активных процессов, которые Kaspersky Embedded Systems Security может запустить
       - Количество процессов для постоянной защиты компьютера
       - Количество рабочих процессов для фоновых задач проверки по требованию
   - В разделе **Взаимодействие с пользователем** настройте отображение значка области уведомлений в панели задач при каждом запуске программы.
   - На закладке **Безопасность и надежность** можно настроить следующие параметры:
     - В разделе **Параметры надежности** укажите количество попыток восстановления задачи проверки по требованию после ее аварийного завершения.
   - В разделе **Действия при переходе на источник бесперебойного питания** укажите действия Kaspersky Embedded Systems Security при переходе на источник бесперебойного питания.
   - В разделе **Параметры применения пароля** настройте параметры защиты паролем функций программы.
   - На закладке **Параметры соединения**:
     - В разделе **Параметры прокси-сервера** укажите параметры прокси-сервера.
     - В разделе **Параметры аутентификации на прокси-сервере** укажите тип аутентификации и данные, необходимые для аутентификации на прокси-сервере.
     - В разделе **Лицензирование** укажите, будет ли Kaspersky Security Center использоваться в качестве прокси-сервера для активации программы.
   - На закладке **Диагностика сбоев**:

- Если вы хотите записывать отладочную информацию в файл, установите флажок **Записывать отладочную информацию в файл трассировки**.
  - В поле ниже укажите папку, в которую Kaspersky Embedded Systems Security будет сохранять файлы трассировки.
  - Настройте уровень детализации отладочной информации.
  - Укажите максимальный размер файлов трассировки.
  - Укажите максимальное количество файлов в одном журнале трассировки. Kaspersky Embedded Systems Security создает не более указанного максимального количества файлов трассировки для каждого отлаживаемого компонента.
  - Укажите компоненты для отладки.
- Если вы хотите, чтобы программа создавала файл дампа, установите флажок **Создавать во время сбоя файл дампа**.

Kaspersky Embedded Systems Security не отправляет файлы трассировки и файлы дампов автоматически. Диагностические данные могут быть отправлены только пользователем с соответствующими правами.

- В поле ниже укажите папку, в которую Kaspersky Embedded Systems Security будет сохранять файл дампа.

Kaspersky Embedded Systems Security записывает информацию в файлы трассировки и файлы дампов в незашифрованном виде. Папка, в которую сохраняются файлы, выбирается пользователем и контролируется параметрами операционной системы и Kaspersky Embedded Systems Security. Можно настроить права доступа и разрешить доступ к журналам, файлам трассировки и файлам дампов только для выбранных пользователей.

3. Нажмите на кнопку **OK**.

Параметры работы Kaspersky Embedded Systems Security будут сохранены.

Управление задачами Kaspersky Embedded Systems Security

Этот раздел содержит информацию о задачах Kaspersky Embedded Systems Security, их создании, настройке параметров выполнения, запуске и остановке.

Категории задач Kaspersky Embedded Systems Security

Функции постоянной защиты компьютера, контроля компьютера, проверки по требованию и обновления в Kaspersky Embedded Systems Security реализованы в виде задач.

Вы можете управлять задачами с помощью контекстного меню задачи в дереве Консоли программы, панели инструментов и панели быстрого доступа. Вы можете просматривать информацию о состоянии задачи в панели результатов. Операции по управлению задачами регистрируются в журнале системного аудита.

Существует два типа задач Kaspersky Embedded Systems Security: *локальные* и *групповые*.

Локальные задачи

Локальные задачи выполняются только на том защищаемом устройстве, для которого они созданы. В зависимости от способа запуска существуют следующие типы локальных задач:

- **Локальные системные задачи**. Создаются автоматически при установке Kaspersky Embedded Systems Security. Вы можете изменять параметры всех системных задач, кроме задач Проверка объектов на карантине и Откат обновления баз программы. Вы не можете переименовывать или удалять системные задачи. Вы можете запускать системные и пользовательские задачи проверки по требованию одновременно.

- **Локальные пользовательские задачи**. В Консоли программы вы можете создавать задачи проверки по требованию. В Kaspersky Security Center вы можете создавать задачи проверки по требованию, обновления баз программы, отката обновления баз программы и копирования обновлений. Такие задачи называются пользовательскими. Вы можете переименовывать, настраивать и удалять пользовательские задачи. Вы можете запускать несколько пользовательских задач одновременно.

Групповые задачи

Групповые задачи и задачи для наборов управляемых устройств, созданные через Kaspersky Security Center, отображаются в Консоли программы. Такие задачи называются групповыми. Вы можете управлять групповыми задачами и настраивать их из программы Kaspersky Security Center. В Консоли программы можно только просматривать состояние групповых задач.

Запуск / приостановка / возобновление / остановка задачи вручную

Вы можете приостанавливать и возобновлять только задачи постоянной защиты компьютера и проверки по требованию.

Чтобы запустить / приостановить / возобновить / остановить задачу, выполните следующие действия:

1. Откройте контекстное меню задачи в Консоли программы.

2. Выберите один из следующих вариантов: **Запустить**, **Приостановить**, **Возобновить** или **Остановить**.

   Операция будет выполнена и зарегистрирована в журнале системного аудита.

После возобновления задачи проверки по требованию Kaspersky Embedded Systems Security продолжает проверку с того объекта, на котором выполнение задачи было приостановлено.

Работа с расписанием задач

Можно настроить расписание запуска задач Kaspersky Embedded Systems Security, а также настроить параметры запуска по расписанию.

Настройка расписания запуска задач

В Консоли программы вы можете настроить расписание запуска локальных системных и пользовательских задач. Вы не можете настраивать расписание запуска групповых задач.

Чтобы настроить расписание запуска задачи, выполните следующие действия:

1. Откройте контекстное меню задачи, для которой вы хотите настроить расписание запуска.
2. Выберите пункт **Свойства**.

   Откроется окно **Параметры задачи**.
3. В открывшемся окне на закладке **Расписание** установите флажок **Запускать задачу по расписанию**.
4. Настройте параметры расписания в соответствии с вашими требованиями. Для этого выполните следующие действия:

   a. В раскрывающемся списке **Частота запуска** выберите одно из следующих значений:

   - **Ежечасно**, если вы хотите, чтобы задача запускалась периодически через заданное количество часов, и укажите количество часов в поле **Раз в <количество> ч**.
   - **Ежесуточно**, если вы хотите, чтобы задача запускалась периодически через заданное количество дней, и укажите количество дней в поле **Раз в <количество> сут**.
   - **Еженедельно**, если вы хотите, чтобы задача запускалась периодически через заданное количество недель, и укажите количество недель в поле **Раз в <количество> нед. по**. Укажите, по каким дням недели будет запускаться задача (по умолчанию задача запускается по понедельникам).
   - **При запуске программы**, если вы хотите, чтобы задача запускалась при каждом запуске Kaspersky Embedded Systems Security.
   - **После обновления баз программы**, если вы хотите, чтобы задача запускалась после каждого обновления баз программы.

   b. В поле **Время запуска** укажите время первого запуска задачи.

   c. В поле **Начать с** укажите дату начала действия расписания.

   После того как вы укажете частоту и время первого запуска задачи и дату начала действия расписания, в верхней части окна в поле **Следующий запуск** отобразится расчетное время очередного запуска задачи. Расчетное время следующего запуска задачи будет обновляться каждый раз, когда вы открываете окно **Параметры задачи** на закладке **Расписание**.

   Значение **Запрещен политикой** отображается в поле **Следующий запуск**, если параметрами политики Kaspersky Security Center запрещен запуск системных задач по расписанию.

5. На закладке **Дополнительно** настройте следующие параметры расписания в соответствии с вашими требованиями.

   - В блоке **Параметры остановки задачи**:

     a. Установите флажок **Длительность** и в полях справа укажите максимальную длительность выполнения задачи (количество часов и минут).

     b. Установите флажок **Приостановить с** и в полях справа укажите начальное и конечное значение временного промежутка в пределах суток, в течение которого выполнение задачи будет приостановлено.

   - В блоке **Дополнительные параметры**:

     a. Установите флажок **Отменить расписание с** и укажите дату, начиная с которой расписание перестанет действовать.

     b. Установите флажок **Запускать пропущенные задачи**, чтобы включить запуск пропущенных задач.

     c. Установите флажок **Распределить время запуска в интервале** и укажите значение параметра в минутах.

6. Нажмите на кнопку **OK**.

Настроенные параметры расписания запуска выбранной задачи будут сохранены.

Включение и выключение запуска задач по расписанию

Вы можете включать и выключать запуск задач по расписанию как после, так и до настройки параметров расписания.

Чтобы включить или выключить расписание запуска задачи, выполните следующие действия:

1. В дереве Консоли программы откройте контекстное меню задачи, для которой вы хотите настроить расписание запуска.
2. Выберите пункт **Свойства**.

   Откроется окно **Параметры задачи**.
3. В открывшемся окне на закладке **Расписание** выполните одно из следующих действий:

   - Установите флажок **Запускать задачу по расписанию**, если вы хотите включить запуск задачи по расписанию.
   - Снимите флажок **Запускать задачу по расписанию**, если вы хотите выключить запуск задачи по расписанию.

     Настроенные параметры расписания запуска задачи не будут удалены и применятся при следующем включении запуска задачи по расписанию.
4. Нажмите на кнопку **OK**.

Настроенные параметры запуска задачи по расписанию будут сохранены.

Использование учетных записей для запуска задач

Вы можете запускать задачи, используя системную учетную запись пользователя или указать другую учетную запись.

Об использовании учетных записей для запуска задач

Вы можете указать учетную запись, с правами которой вы хотите запускать выбранную задачу, для следующих функциональных компонентов Kaspersky Embedded Systems Security:

- задачи Формирование правил контроля запуска программ и Формирование правил контроля устройств;
- задачи проверки по требованию;
- задачи обновления.

По умолчанию указанные задачи выполняются с правами системной учетной записи.

Рекомендуется указать другую учетную запись с достаточными правами доступа в следующих случаях:

- в задаче обновления, если в качестве источника обновления вы указали папку общего доступа на другом устройстве в сети;
- в задаче обновления, если для доступа к источнику обновлений используется прокси-сервер со встроенной в Windows проверкой подлинности NTLM;
- в задачах проверки по требованию, если системная учетная запись не обладает правами доступа к проверяемым объектам (например, к файлам в папках общего доступа на защищаемом устройстве);
- в задаче Формирование правил контроля запуска программ, если после выполнения задачи сформированные правила экспортируются в конфигурационный файл, недоступный для системной учетной записи (например, расположенный в одной из папок общего доступа на защищаемом устройстве).

Вы можете запускать задачи обновления, проверки по требованию и автоматического формирования разрешающих правил контроля запуска программ с правами системной учетной записи. В ходе выполнения этих задач Kaspersky Embedded Systems Security обращается к папкам общего доступа на другом устройстве в сети, если это устройство зарегистрировано в одном домене с защищаемым устройством. В этом случае системная учетная запись должна обладать правами доступа к этим папкам. Kaspersky Embedded Systems Security будет обращаться к устройству с правами учетной записи **<имя домена \ имя компьютера>**.

Указание учетной записи для запуска задачи

Чтобы указать учетную запись для запуска задачи, выполните следующие действия:

1. В дереве Консоли программы откройте контекстное меню задачи, которую вы хотите запустить с правами определенной учетной записи.
2. Выберите пункт **Свойства**.

   Откроется окно **Параметры задачи**.
3. В открывшемся окне на закладке **Запуск с правами** выполните следующие действия:

   a. Выберите вариант **Имя пользователя**.

   b. Укажите имя и пароль пользователя, учетную запись которого вы хотите использовать.

   > Выбранный пользователь должен быть зарегистрирован на защищаемом устройстве или в одном домене с защищаемым устройством.

   c. Подтвердите введенный пароль.
4. Нажмите на кнопку **OK**.

Измененные параметры запуска задачи с правами учетной записи будут сохранены.

Импорт и экспорт параметров

В этом разделе приведена информация об экспорте параметров Kaspersky Embedded Systems Security или параметров определенных программных компонентов в конфигурационный файл в формате XML и об импорте этих параметров из конфигурационного файла в программу.

Об импорте и экспорте параметров

Вы можете экспортировать параметры Kaspersky Embedded Systems Security в конфигурационный файл в формате XML и импортировать параметры в Kaspersky Embedded Systems Security из конфигурационного файла. Вы можете сохранить в конфигурационный файл как все параметры программы, так и параметры ее отдельных компонентов.

Когда вы экспортируете все параметры Kaspersky Embedded Systems Security, в файл сохраняются общие параметры программы и параметры следующих компонентов и функций Kaspersky Embedded Systems Security:

- Постоянная защита файлов
- Использование KSN
- Контроль устройств
- Контроль запуска программ
- Формирование правил контроля устройств
- Формирование правил контроля запуска программ

- Задачи проверки по требованию
- Мониторинг файловых операций
- Анализ журналов
- Обновление баз и модулей Kaspersky Embedded Systems Security
- Карантин
- Резервное хранилище
- Журналы
- Уведомления администратора и пользователей
- Доверенная зона
- Защита от эксплойтов
- Защита паролем

Также вы можете сохранять в файле общие параметры Kaspersky Embedded Systems Security и права учетных записей пользователей.

Вы не можете экспортировать параметры групповых задач.

Kaspersky Embedded Systems Security экспортирует все пароли, используемые в программе, например, параметры учетных записей для запуска задач или соединения с прокси-сервером. Экспортированные пароли хранятся в конфигурационном файле в зашифрованном виде. Пароли можно импортировать только с помощью программы Kaspersky Embedded Systems Security, установленной на этом же защищаемом устройстве, если она не была переустановлена или обновлена.

Нельзя импортировать ранее сохраненные пароли с помощью программы Kaspersky Embedded Systems Security, установленной на другом защищаемом устройстве. После импорта параметров на другом защищаемом устройстве нужно ввести все пароли вручную.

Если в момент экспорта параметров действует политика Kaspersky Security Center, программа экспортирует значения, применяемые политикой.

Можно импортировать параметры из конфигурационного файла, содержащего параметры только отдельных компонентов Kaspersky Embedded Systems Security (например, созданного в программе Kaspersky Embedded Systems Security, установленной с неполным набором компонентов). После импорта параметров в Kaspersky Embedded Systems Security изменяются только те параметры, которые содержались в конфигурационном файле. Остальные параметры не изменяются.

Заблокированные параметры активной политики Kaspersky Security Center при импорте параметров не изменяются.

Экспорт параметров

Чтобы экспортировать параметры в конфигурационный файл, выполните следующие действия:

1. В дереве Консоли программы выполните одно из следующих действий:

   - В контекстном меню узла **Kaspersky Embedded Systems Security** выберите пункт **Экспортировать параметры**, чтобы экспортировать все параметры Kaspersky Embedded Systems Security.

   - В контекстном меню задачи, параметры которой вы хотите экспортировать, выберите пункт **Экспортировать параметры**, чтобы экспортировать параметры отдельного функционального компонента программы.

   - Чтобы экспортировать параметры компонента Доверенная зона:

     a. В дереве Консоли программы откройте контекстное меню узла **Kaspersky Embedded Systems Security**.

     b. Выберите пункт **Настроить параметры доверенной зоны**.

     Откроется окно **Доверенная зона**.

     c. Нажмите на кнопку **Экспорт**.

     Откроется окно приветствия мастера экспорта параметров.

2. Выполните инструкции, которые предлагает **Мастер экспорта параметров программы**: задайте имя и путь конфигурационного файла для сохранения параметров.

   Указывая путь, вы можете использовать системные переменные окружения, но не можете использовать пользовательские переменные окружения.

   Если в момент экспорта параметров действует политика Kaspersky Security Center, программа экспортирует параметры, используемые в политике.

3. В окне **Экспорт параметров программы завершен** нажмите на кнопку **Закрыть**.

Мастер экспорта параметров будет закрыт; экспорт параметров будет завершен.

Импорт параметров

Чтобы импортировать параметры из сохраненного конфигурационного файла, выполните следующие действия:

1. В дереве Консоли программы выполните одно из следующих действий:

   - В контекстном меню узла **Kaspersky Embedded Systems Security** выберите пункт **Импортировать параметры**, чтобы импортировать все параметры Kaspersky Embedded Systems Security.

   - В контекстном меню задачи, параметры которой вы хотите импортировать, выберите пункт **Импортировать параметры**, чтобы импортировать параметры отдельного функционального компонента.

   - Чтобы импортировать параметры компонента Доверенная зона:

     a. В дереве Консоли программы откройте контекстное меню узла **Kaspersky Embedded Systems Security**.

     b. Выберите пункт **Настроить параметры доверенной зоны**.

Откроется окно **Доверенная зона**.

c. Нажмите на кнопку **Импорт**.

Откроется окно приветствия мастера импорта параметров.

2. Выполните инструкции, которые предлагает **Мастер импорта параметров программы**: укажите конфигурационный файл, из которого вы хотите импортировать параметры.

После импорта общих параметров или функциональных компонентов Kaspersky Embedded Systems Security на защищаемое устройство, будет невозможно восстановить их прежние значения.

3. В окне **Импорт параметров программы завершен** нажмите на кнопку **Закрыть**.

Мастер импорта параметров будет закрыт; импортированные параметры будут сохранены.

4. В панели инструментов Консоли программы нажмите на кнопку **Обновить**.

Импортированные параметры отобразятся в окне Консоли программы.

Kaspersky Embedded Systems Security не импортирует пароли (учетные данные для запуска задач или для соединения с прокси-сервером) из файла, созданного на другом защищаемом устройстве или на этом же защищаемом устройстве, после того как на нем была переустановлена или обновлена программа Kaspersky Embedded Systems Security. После завершения импорта вам нужно ввести пароли вручную.

Использование шаблонов параметров безопасности

Этот раздел содержит информацию о работе с шаблонами параметров безопасности в задачах защиты и проверки Kaspersky Embedded Systems Security.

О шаблонах параметров безопасности

Вы можете вручную настроить параметры безопасности узла в дереве или списке файловых ресурсов защищаемого устройства и сохранить значения настроенных параметров в шаблон. Затем вы можете применить этот шаблон при настройке параметров безопасности других узлов в задачах защиты и проверки Kaspersky Embedded Systems Security.

Использование шаблонов доступно при настройке параметров безопасности следующих задач Kaspersky Embedded Systems Security:

- Постоянная защита файлов
- Проверка при старте операционной системы
- Проверка важных областей
- Задачи проверки по требованию

Значения параметров безопасности из шаблона, примененного к родительскому узлу в дереве файловых ресурсов защищаемого устройства, распространяются на все вложенные узлы. Шаблон родительского узла не применяется к вложенным узлам в следующих случаях:

- Если параметры безопасности вложенных узлов настраивались отдельно.
- Если вложенные узлы виртуальные. Вам нужно применить шаблон для каждого виртуального узла отдельно.

Создание шаблона параметров безопасности

Чтобы сохранить параметры безопасности узла вручную в шаблон, выполните следующие действия:

1. В дереве Консоли программы выберите задачу, для которой вы хотите создать шаблон параметров безопасности.
2. В панели результатов выбранной задачи перейдите по ссылке **Настроить область защиты** или **Настроить область проверки**.
3. В дереве или в списке сетевых файловых ресурсов защищаемого устройства выберите шаблон, который вы хотите просмотреть.
4. На закладке **Уровень безопасности** нажмите на кнопку **Сохранить как шаблон**.

   Откроется окно **Свойства шаблона**.
5. В поле **Название шаблона** введите название шаблона.
6. В поле **Описание** введите дополнительную информацию о шаблоне.
7. Нажмите на кнопку **ОК**.

Шаблон с набором значений параметров безопасности будет сохранен.

Просмотр параметров безопасности в шаблоне

Чтобы просмотреть значения параметров безопасности в созданном шаблоне, выполните следующие действия:

1. В дереве Консоли программы выберите задачу, для которой вы хотите просмотреть шаблон параметров безопасности.
2. В контекстном меню выбранной задачи выберите пункт **Шаблоны параметров**.

   Откроется окно **Шаблоны**.
3. В открывшемся окне в списке шаблонов выберите шаблон, который вы хотите просмотреть.
4. Нажмите на кнопку **Просмотреть**.

Откроется окно **<Название шаблона>**. На закладке **Общие** отображается имя шаблона и дополнительная информация о шаблоне; на закладке **Параметры** приведен список параметров безопасности, сохраненных в шаблоне.

Применение шаблона параметров безопасности

Чтобы применить параметры безопасности из шаблона к выбранному узлу, выполните следующие действия:

1. В дереве Консоли программы выберите задачу, к которой вы хотите применить шаблон параметров безопасности.
2. В панели результатов выбранной задачи перейдите по ссылке **Настроить область защиты** или **Настроить область проверки**.
3. В дереве или списке сетевых файловых ресурсов защищаемого устройства откройте контекстное меню узла или элемента, к которому вы хотите применить шаблон.
4. Выберите **Применить шаблон** → **<Название шаблона>**.
5. Нажмите на кнопку **Сохранить**.

   Шаблон параметров безопасности будет применен к выбранному узлу в дереве файловых ресурсов защищаемого устройства. На закладке **Уровень безопасности** выбранного узла будет установлено значение **Другой**.

Значения параметров безопасности из шаблона, примененного к родительскому узлу в дереве файловых ресурсов защищаемого устройства, распространяются на все вложенные узлы.

Если область защиты или область проверки вложенных узлов в дереве файловых ресурсов устройства настраивалась отдельно, параметры безопасности из шаблона, примененного к родительскому узлу, не применяются автоматически к таким вложенным узлам.

Чтобы применить параметры безопасности из шаблона ко всем выбранным узлам, выполните следующие действия:

1. В дереве Консоли программы выберите задачу, к которой вы хотите применить шаблон параметров безопасности.
2. В панели результатов выбранной задачи перейдите по ссылке **Настроить область защиты** или **Настроить область проверки**.
3. В дереве или в списке сетевых файловых ресурсов защищаемого устройства выберите родительский узел, чтобы применить шаблон к этому узлу и ко всем его вложенным узлам.
4. В контекстном меню выберите пункт **Применить шаблон** → **<Название шаблона>**.
5. Нажмите на кнопку **Сохранить**.

   Шаблон параметров безопасности будет применен к родительскому и всем вложенным узлам в дереве файловых ресурсов защищаемого устройства. На закладке **Уровень безопасности** выбранного узла будет установлено значение **Другой**.

Удаление шаблона параметров безопасности

Чтобы удалить шаблон параметров безопасности, выполните следующие действия:

1. В дереве Консоли программы выберите задачу, для настройки которой больше не требуется использовать шаблон параметров безопасности.
2. В контекстном меню выбранной задачи выберите пункт **Шаблоны параметров**.

   Вы можете просмотреть шаблоны параметров для задач проверки по требованию из панели результатов родительского узла **Проверка по требованию**.

   Откроется окно **Шаблоны**.
3. В открывшемся окне в списке шаблонов выберите шаблон, который вы хотите удалить.
4. Нажмите на кнопку **Удалить**.

   Откроется окно подтверждения операции удаления.
5. В открывшемся окне нажмите на кнопку **Да**.

Выбранный шаблон будет удален.

Если шаблон параметров безопасности применялся для защиты или проверки узлов в дереве файловых ресурсов устройства, настроенные для этих узлов параметры безопасности сохраняются после удаления шаблона.

Просмотр состояния защиты и информации о Kaspersky Embedded Systems Security

Чтобы просмотреть информацию о состоянии защиты устройства в Kaspersky Embedded Systems Security,

в дереве Консоли программы выберите узел **Kaspersky Embedded Systems Security**.

По умолчанию информация в панели результатов Консоли программы обновляется автоматически:

- каждые 10 секунд при локальном подключении;
- каждые 15 секунд при удаленном подключении.

Вы можете обновлять информацию вручную.

*Чтобы вручную обновить информацию в узле **Kaspersky Embedded Systems Security**,*

в контекстном меню узла **Kaspersky Embedded Systems Security** выберите пункт **Обновить**.

В панели результатов Консоли программы отображается следующая информация о программе:

- статус использования Kaspersky Security Network;

- состояние защиты устройства;
- данные об обновлении баз и модулей программы;
- актуальные данные диагностики;
- данные о задачах контроля защищаемого устройства;
- данные о лицензии;
- статус интеграции с Kaspersky Security Center: данные сервера с установленной программой Kaspersky Security Center, к которому подключена программа; данные о контроле задач программы активной политикой.

Для отображения состояния защиты используется цветовая индикация:

- *Зеленый цвет*. Задача выполняется в соответствии с настроенными параметрами. Защита обеспечивается.
- *Желтый цвет*. Задача не запущена, приостановлена или остановлена. Возможно возникновение угрозы безопасности. Рекомендуется настроить и запустить задачу.
- *Красный цвет*. Задача завершена с ошибкой или при работе задачи была обнаружена угроза безопасности. Рекомендуется запустить задачу или принять меры по устранению обнаруженной угрозы безопасности.

Часть информации в блоке (например, названия задач или количество обнаруженных угроз) являются ссылками, по которым вы можете перейти в узел соответствующей задачи или открыть журнал ее выполнения.

В разделе **Использование Kaspersky Security Network** отображается текущий статус задачи, например, *Выполняется*, *Остановлена* или *Не выполнялась*. Индикатор может принимать следующие значения:

- Зеленый – задача Использование KSN выполняется и запросы о файловой репутации отправляются в KSN.
- Желтый – принято одно из Положений, но задача не выполняется, или задача выполняется, но запросы не отправляются в KSN.

Защита компьютера

В разделе **Защита компьютера** (см. таблицу ниже) отображается информация о текущем состоянии защиты устройства.

Информация о состоянии защиты устройства

Раздел Защита	Информация
Индикатор состояния защиты устройства	Цвет панели с названием блока является индикатором состояния задач, выполняемых в этом блоке. Индикатор может принимать следующие значения: • Зеленый – отображается по умолчанию и означает, что компонент Постоянная защита файлов установлен и задача выполняется. • Желтый – компонент Постоянная защита файлов не установлен и задача Проверка важных областей не выполнялась в течение долгого времени.

	• Красный – задача Постоянная защита файлов не выполняется.
Постоянная защита файлов	**Статус задачи** – текущее состояние задачи, например, *Выполняется* или *Остановлена*. **Обнаружено** – количество объектов, обнаруженных программой Kaspersky Embedded Systems Security. Например, если программа Kaspersky Embedded Systems Security обнаружила одну вредоносную программу в пяти файлах, значение в этом поле увеличится на единицу. Если количество обнаруженных вредоносных программ больше 0, значение выделяется красным цветом.
Проверка важных областей	**Дата последней проверки** – дата и время последней проверки важных областей компьютера на наличие вирусов и других угроз безопасности. *Не выполнялась* – событие, которое возникает, если задача Проверка важных областей выполнялась 30 и более дней назад (по умолчанию). Вы можете изменять порог формирования этого события.
Защита от эксплойтов	**Статус** – текущий статус функции защиты от эксплойтов, например, *Используется* или *Не применяется*. **Режим работы** – один из двух доступных режимов, выбранный при настройке защиты памяти процессов: **Завершать скомпрометированные процессы** или **Только статистика**. **Процессов защищено** – общее количество процессов, которые были добавлены в область защиты и обрабатываются в соответствие с выбранным режимом.
Объектов в резервном хранилище	*Превышен порог доступного пространства в резервном хранилище* – событие, которое возникает, если объем доступного пространства в резервном хранилище достигает указанного значения. Kaspersky Embedded Systems Security при этом продолжает помещать объекты в резервное хранилище. В этом случае значение в поле **Используемое пространство** выделяется желтым цветом. *Превышен максимальный размер резервного хранилища* – событие, которое возникает, если размер резервного хранилища достигает указанного значения. Kaspersky Embedded Systems Security при этом продолжает помещать объекты в резервное хранилище. В этом случае значение в поле **Используемое пространство** выделяется красным цветом. **Объектов в резервном хранилище** – количество объектов, находящихся в резервном хранилище. **Используемое пространство** – объем используемого пространства в резервном хранилище.

Обновление

В разделе **Обновление** (см. таблицу ниже) отображается информация об актуальности баз и модулей программы.

Информация о состоянии баз и модулей Kaspersky Embedded Systems Security

Раздел Обновление	Информация
Индикатор состояния баз и модулей программы	Цвет панели с названием блока является индикатором состояния баз и модулей программы. Индикатор может принимать следующие значения: • Зеленый – отображается по умолчанию и означает, что базы программы актуальны и последняя задача обновления баз программы завершена успешно. • Желтый – базы программы устарели или последняя задача Обновление баз программы завершена с ошибкой.

	• Красный – возникло событие *Базы программы сильно устарели* или *Базы программы повреждены*.
Обновление баз программы и **Обновление модулей программы**	**Актуальность баз программы** – оценка статуса Обновления баз программы. Параметр может принимать следующие значения: • **Базы программы актуальны** – базы программы были обновлены не более чем 7 дней назад (по умолчанию). • **Базы программы устарели** – базы программы были обновлены от 7 до 14 дней назад (по умолчанию). • **Базы программы сильно устарели** – базы программы были обновлены более чем 14 дней назад (по умолчанию). Вы можете изменять пороги формирования событий *Базы программы устарели* и *Базы программы сильно устарели*. **Дата выпуска баз программы** – дата и время выпуска последнего обновления баз программы. Дата и время указаны в UTC-формате. **Статус последней запущенной задачи обновления баз программы** – дата и время последнего обновления баз программы. Дата и время указаны по местному времени защищаемого устройства. Поле окрашивается в красный цвет, если возникло событие *Завершена с ошибкой*. **Доступно обновлений модулей программы** – количество обновлений модулей Kaspersky Embedded Systems Security, доступных для загрузки и установки. **Установлено обновлений модулей программы** – количество установленных обновлений модулей Kaspersky Embedded Systems Security.

Контроль

В разделе **Контроль** (см. таблицу ниже) отображается информация о задачах Контроль запуска программ, Контроль устройств и Управление сетевым экраном.

Информация о состоянии контроля защищаемого устройства

Раздел Контроль	Информация
Индикатор состояния контроля защищаемого устройства	Цвет панели с названием блока является индикатором состояния задач, выполняемых в этом блоке. Индикатор может принимать следующие значения: • Зеленый – отображается по умолчанию и означает, что компонент Контроль запуска программ установлен и задача выполняется в режиме активном **Активный**. • Желтый – задача Контроль запуска программ выполняется в режиме **Только статистика**. • Красный – задача Контроль запуска программ не выполняется или завершена с ошибкой.
Контроль запуска программ	**Статус задачи** – текущее состояние задачи, например, *Выполняется* или *Остановлена*. **Режим работы** – один из двух доступных режимов работы задачи Контроль запуска программ: **Активный** или **Только статистика**.

	Заблокировано запусков программ – количество попыток запуска программ, заблокированных Kaspersky Embedded Systems Security в ходе выполнения задачи Контроль запуска программ. Если количество заблокированных запусков программ превышает 0, поле окрашивается в красный цвет. **Среднее время обработки (мс)** – время, которое потребовалось Kaspersky Embedded Systems Security для обработки попытки запуска программ на защищаемом устройства.
Контроль устройств	**Статус задачи** – текущее состояние задачи, например, *Выполняется* или *Остановлена*. **Режим работы** – один из двух доступных режимов работы задачи Контроль устройств: **Активный** или **Только статистика**. **Заблокировано устройств** – количество попыток подключения внешних устройств, заблокированных Kaspersky Embedded Systems Security в ходе выполнения задачи Контроль устройств. Если количество заблокированных внешних устройств превышает 0, значение поля окрашивается в красный цвет.
Управление сетевым экраном	**Статус задачи** – текущее состояние задачи, например, *Выполняется* или *Остановлена*. **Заблокировано попыток подключения** – количество подключений к защищаемому устройству, которые не были разрешены заданными правилами сетевого экрана.

Диагностика

В разделе **Диагностика** (см. таблицу ниже) отображается информация о задачах Мониторинг файловых операций и Анализ журналов.

Информация о состоянии диагностики системы

Раздел Диагностика	Информация
Индикатор статуса диагностики	Цвет панели с названием блока является индикатором состояния задач, выполняемых в этом блоке. Индикатор может принимать следующие значения: • Зеленый – отображается по умолчанию и означает, что один или оба компонента диагностики системы установлены и задачи выполняются. • Желтый – оба компонента установлены, но одна из задач диагностики системы не выполняется; возникает событие *Не выполняется*. • Красный – одна из задач завершена с ошибкой.
Мониторинг файловых операций	**Статус задачи** – текущее состояние задачи, например, *Выполняется* или *Остановлена*. **Несанкционированных файловых операций** – количество изменений в файлах из области мониторинга. Эти изменения могут указывать на нарушение безопасности защищаемого устройства.
Анализ журналов	**Статус задачи** – текущее состояние задачи, например, *Выполняется* или *Остановлена*. **Возможных нарушений** – количество зафиксированных нарушений по данным журнала событий Windows. Это количество определяется на основе заданных правил задачи или применения эвристического анализатора.

Информация о лицензии на Kaspersky Embedded Systems Security отображается в строке в левом нижнем углу панели результатов узла **Kaspersky Embedded Systems Security**.

Вы можете настроить свойства Kaspersky Embedded Systems Security, перейдя по ссылке **Свойства программы**.

Вы можете подключиться к другому защищаемому устройству, перейдя по ссылке **Подключиться к другому компьютеру**.

Работа с Веб-плагином

Этот раздел содержит информацию о Плагине управления Kaspersky Embedded Systems Security и об управлении программой, установленной на защищаемом устройстве или группе защищаемых устройств.

Управление Kaspersky Embedded Systems Security из Kaspersky Security Center Web Console

Вы можете централизованно управлять несколькими защищаемыми устройствами с установленной программой Kaspersky Embedded Systems Security, объединенными в группу администрирования, с помощью Веб-плагина Kaspersky Embedded Systems Security. Kaspersky Security Center Web Console также позволяет отдельно настраивать параметры работы для каждого защищаемого устройства, входящего в группу администрирования.

Группа администрирования формируется вручную на стороне Kaspersky Security Center Web Console и включает несколько устройств с установленной программой Kaspersky Embedded Systems Security, для которых вы хотите настроить единые параметры управления и защиты. Подробная информация об использовании групп администрирования приведена в *Справке Kaspersky Security Center*.

Параметры программы для отдельного защищаемого устройства недоступны для настройки, если работа Kaspersky Embedded Systems Security на этом защищаемом устройстве контролируется активной политикой Kaspersky Security Center.

Вы можете управлять Kaspersky Embedded Systems Security из Kaspersky Security Center Web Console следующими способами:

- **С помощью политик Kaspersky Security Center**. Политики Kaspersky Security Center позволяют удаленно настроить единые параметры защиты для группы устройств. Параметры задачи, указанные в активной политике, имеют приоритет над параметрами задачи, настроенными локально в Консоли программы или удаленно в окне свойств устройства в Kaspersky Security Center Web Console.

  С помощью политик вы можете настроить общие параметры работы программы, параметры задач постоянной защиты, контроля активности на компьютерах, а также параметры запуска системных задач по расписанию.

- **С помощью групповых задач Kaspersky Security Center**. Групповые задачи Kaspersky Security Center позволяют удаленно настраивать единые параметры задач, имеющих ограниченный срок выполнения, для группы устройств.

- С помощью групповых задач вы можете активировать программу, настроить параметры задач проверки по требованию, параметры задач обновления и параметры задачи формирования правил контроля запуска программ.

- **С помощью задач для набора устройств**. Задачи для набора устройств позволяют удаленно настраивать единые параметры задач, имеющих ограниченный срок выполнения, для защищаемых устройств, не входящих ни в одну группу администрирования.

- **С помощью окна свойств отдельного устройства**. В окне свойств устройства можно удаленно настроить параметры задачи для отдельного защищаемого устройства, включенного в группу администрирования. Вы можете настроить как общие параметры работы программы, так и параметры работы всех задач Kaspersky Embedded Systems Security, если выбранное защищаемое устройство не находится под управлением активной политики Kaspersky Security Center.

Kaspersky Security Center Web Console позволяет настроить параметры программы, дополнительные возможности и работу журналов и уведомлений. Вы можете настроить эти параметры как для группы защищаемых устройств, так и для отдельного защищаемого устройства.

Ограничения Веб-плагина

Веб-плагин Kaspersky Embedded Systems Security имеет следующие ограничения по сравнению с Плагином управления Kaspersky Embedded Systems Security:

- Чтобы добавить пользователей и группы пользователей, необходимо указать строки дескриптора безопасности с помощью языка описания дескрипторов безопасности (SDDL).
- Для задачи Постоянная защита файлов нельзя изменить стандартный уровень безопасности.
- Для задачи Контроль запуска программ нельзя сформировать правила на основе цифрового сертификата или событий Kaspersky Security Center.
- Для задачи Контроль устройств нельзя сформировать правила на основе подключенных устройств или данных системы.

Управление параметрами программы

Этот раздел содержит информацию о настройке общих параметров работы Kaspersky Embedded Systems Security в Kaspersky Security Center Web Console.

Настройка общих параметров программы в Kaspersky Security Center Web Console

Вы можете настроить общие параметры Kaspersky Embedded Systems Security из Kaspersky Security Center для группы защищаемых устройств или для отдельного защищаемого устройства.

Настройка масштабируемости и интерфейса в Kaspersky Security Center Web Console

Чтобы настроить параметры масштабируемости и интерфейс программы, выполните следующие действия:

1. В главном окне веб-консоли выберите **Устройства** → **Политики и профили**.
2. Выберите политику, которую вы хотите настроить.
3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.
4. Перейдите в раздел **Параметры программы**.
5. Нажмите на кнопку **Параметры** в подразделе **Масштабируемость и интерфейс**.

6. Настройте параметры, приведены в следующей таблице.

Параметры масштабируемости

Параметр	Описание
Определять параметры масштабируемости автоматически	Kaspersky Embedded Systems Security автоматически регулирует количество используемых процессов. Это значение установлено по умолчанию.
Указать количество рабочих процессов вручную	Kaspersky Embedded Systems Security контролирует количество активных рабочих процессов в соответствии с указанными значениями.
Максимальное количество активных процессов	Максимальное количество процессов, которые использует Kaspersky Embedded Systems Security. Поле ввода доступно, если выбран вариант **Указать количество рабочих процессов вручную**.
Количество процессов для постоянной защиты	Максимальное количество процессов, которые используют компоненты задач постоянной защиты компьютера. Поле ввода доступно, если выбран вариант **Указать количество рабочих процессов вручную**.
Количество процессов для фоновых задач проверки по требованию	Максимальное количество процессов, которые использует компонент проверки по требованию при выполнении задач проверки по требованию в фоновом режиме. Поле ввода доступно, если выбран вариант **Указать количество рабочих процессов вручную**.
Показывать Значок области уведомлений	Настройте, будет ли Значок области уведомлений отображаться в панели задач
Параметры HSM-системы	Выберите тип доступа к иерархическому хранилищу

Настройка параметров безопасности в Kaspersky Security Center Web Console

Чтобы вручную настроить параметры безопасности, выполните следующие действия:

1. В главном окне веб-консоли выберите **Устройства** → **Политики и профили**.
2. Выберите политику, которую вы хотите настроить.
3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.
4. Перейдите в раздел **Параметры программы**.
5. Нажмите на кнопку **Параметры** в подразделе **Безопасность**.
6. Настройте параметры, приведены в следующей таблице.

Параметры безопасности

Параметр	Описание
Выполнять восстановление	

задач	Флажок включает или выключает восстановление задач Kaspersky Embedded Systems Security после сбоя в работе программы или аварийного завершения работы программы. Если флажок установлен, Kaspersky Embedded Systems Security автоматически восстанавливает задачи Kaspersky Embedded Systems Security после сбоя в работе программы или аварийного завершения работы программы. Если флажок снят, Kaspersky Embedded Systems Security не восстанавливает задачи Kaspersky Embedded Systems Security после сбоя в работе программы или аварийного завершения работы программы. По умолчанию флажок установлен.
Выполнять восстановление задач проверки по требованию не более (раз), значение в диапазоне от 1 до 10	Количество попыток восстановления задач проверки по требованию после сбоя в работе Kaspersky Embedded Systems Security. Поле ввода доступно, если установлен флажок **Выполнять восстановление задач**.
Не запускать задачи проверки по расписанию	Флажок включает или выключает запуск задач проверки по расписанию при переходе защищаемого устройства на источник бесперебойного питания до восстановления стандартного режима питания. Если флажок установлен, Kaspersky Embedded Systems Security не запускает задачи проверки по расписанию при переходе защищаемого устройства на источник бесперебойного питания до восстановления стандартного режима питания. Если флажок снят, Kaspersky Embedded Systems Security запускает задачи проверки по расписанию вне зависимости от режима питания. По умолчанию флажок установлен.
Остановить выполнение задачи проверки	Флажок включает или выключает выполнение запущенных задач проверки при переходе защищаемого устройства на источник бесперебойного питания. Если флажок установлен, Kaspersky Embedded Systems Security останавливает выполнение запущенных задач проверки при переходе защищаемого устройства на источник бесперебойного питания. Если флажок снят, Kaspersky Embedded Systems Security продолжает выполнение запущенных задач проверки при переходе защищаемого устройства на источник бесперебойного питания. По умолчанию флажок установлен.
Использовать защиту паролем	Установить пароль для защиты доступа к функциям Kaspersky Embedded Systems Security.

Настройка параметров соединения в Kaspersky Security Center Web Console

Настроенные параметры соединения используются для подключения Kaspersky Embedded Systems Security к серверам обновлений и активации, а также при интеграции программ со службами KSN.

Чтобы настроить параметры соединения, выполните следующие действия:

1. В главном окне веб-консоли выберите **Устройства** → **Политики и профили**.
2. Выберите политику, которую вы хотите настроить.
3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.
4. Перейдите в раздел **Параметры программы**.
5. Нажмите на кнопку **Параметры** в подразделе **Масштабируемость и интерфейс**.
6. Настройте параметры, приведены в следующей таблице.

Параметры соединения

Параметр	Описание
Не использовать прокси-сервер	Если выбран этот вариант, Kaspersky Embedded Systems Security не использует прокси-сервер для соединения с службами KSN, а выполняет соединение напрямую.
Использовать параметры указанного прокси-сервера	Если выбран этот вариант, для соединения с KSN Kaspersky Embedded Systems Security использует параметры прокси-сервера, указанные вручную.
Не использовать прокси-сервер для локальных адресов	Флажок включает или выключает использование прокси-сервера при обращении к устройствам в сети, к которой принадлежит защищаемое устройство с установленной программой Kaspersky Embedded Systems Security. Если флажок установлен, обращение к устройствам в сети, к которой принадлежит защищаемое устройство с установленной программой Kaspersky Embedded Systems Security, происходит напрямую. Прокси-сервер не используется. Если флажок снят, для подключения к локальным устройствам используется прокси-сервер. По умолчанию флажок установлен.
Параметры аутентификации на прокси-сервере	Укажите параметры аутентификации
Не использовать аутентификацию	Проверка подлинности не выполняется. Этот режим выбран по умолчанию.
Использовать NTLM-аутентификацию	Проверка подлинности выполняться с помощью протокола сетевой аутентификации NTLM, разработанного компанией Microsoft.
Использовать NTLM-аутентификацию с именем пользователя и паролем	Проверка подлинности выполняется по протоколу сетевой аутентификации NTLM, разработанному компанией Microsoft, с использованием имени пользователя и пароля.
Использовать имя пользователя и пароль	Проверка подлинности выполняется с помощью имени пользователя и пароля.

Настройка запуска по расписанию локальных системных задач

С помощью политик можно разрешать или запрещать запуск локальных системных задач проверки по требованию и обновления по расписанию, настроенному локально на каждом защищаемом устройстве группы администрирования:

- Если запуск по расписанию для локальных системных задач указанных типов запрещен в политике, такие задачи не будут выполняться на защищаемом устройстве по расписанию. Вы можете запустить локальные системные задачи вручную.
- Если запуск по расписанию для локальных системных задач указанного типа разрешен в политике, такие задачи будут выполняться в соответствии с параметрами расписания, настроенными локально для этой задачи.

По умолчанию запуск локальных системных задач запрещается политикой.

Рекомендуется не разрешать запуск локальных системных задач, если обновления или проверки по требованию регулируются с помощью групповых задач Kaspersky Security Center.

Если вы не используете групповые задачи обновления или проверки по требованию, разрешите запуск локальных системных задач в политике: Kaspersky Embedded Systems Security будет выполнять обновления баз и модулей программы, а также запускать все локальные системные задачи проверки по требованию в соответствии с определенным по умолчанию расписанием.

С помощью политик вы можете разрешать или запрещать запуск по расписанию для следующих локальных системных задач:

- Задачи проверки по требованию: Проверка важных областей, Проверка объектов на карантине, Проверка при старте операционной системы, Проверка целостности программы, Мониторинг целостности файлов на основе эталона.
- Задачи обновления: Обновление баз программы, Обновление модулей программы, Копирование обновлений.

Если вы исключите защищаемое устройство из группы администрирования, расписание системных задач будет автоматически включено.

Чтобы разрешить или запретить в политике запуск по расписанию системных задач Kaspersky Embedded Systems Security, выполните следующие действия:

1. В главном окне веб-консоли выберите **Устройства** → **Политики и профили**.
2. Выберите политику, которую вы хотите настроить.
3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.
4. Перейдите в раздел **Параметры программы**.
5. Нажмите на кнопку **Параметры** в подразделе **Запуск системных задач**.
6. Настройте параметры, приведены в следующей таблице.

Параметры запуска системных задач по расписанию

Параметр	Описание
Разрешить запуск задач проверки по требованию	Установите или снимите флажок, чтобы разрешить или запретить запуск по расписанию для задач проверки по требованию
Разрешить запуск задач обновления и копирования обновлений	Установите или снимите флажок, чтобы разрешить или запретить запуск по расписанию для задач обновления и копирования обновлений

Настройка параметров карантина и резервного хранилища с помощью Веб-плагина

Чтобы настроить параметры резервного хранилища в Kaspersky Security Center, выполните следующие действия:

1. В главном окне веб-консоли выберите **Устройства** → **Политики и профили**.
2. Выберите политику, которую вы хотите настроить.
3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.
4. Перейдите в раздел **Параметры программы**.
5. Нажмите на кнопку **Параметры** в подразделе **Запуск системных задач**.
6. Настройте параметры, приведены в следующей таблице.

Параметры запуска системных задач по расписанию

Параметр	Описание
Папка резервного хранилища	Укажите папку резервного хранилища
Максимальный размер резервного хранилища (МБ)	Укажите максимальный размер резервного хранилища
Порог доступного пространства (МБ)	Укажите минимальное значение свободного места в папке резервного хранилища
Папка, в которую восстанавливаются объекты	Укажите папку для восстановленных объектов
Папка карантина	Укажите папку резервного хранилища
Максимальный размер карантина (МБ)	Укажите максимальный размер резервного хранилища
Порог доступного пространства (МБ)	Укажите минимальное значение свободного места в папке резервного хранилища
Папка, в которую восстанавливаются объекты	Укажите папку для восстановленных объектов

Создание и настройка политик

В этом разделе содержится информация о применении политик Kaspersky Security Center для управления Kaspersky Embedded Systems Security на нескольких защищаемых устройствах.

Можно создавать единые политики Kaspersky Security Center для управления защитой нескольких устройств, на которых установлена программа Kaspersky Embedded Systems Security.

Политика применяет указанные в ней значения параметров, функций и задач Kaspersky Embedded Systems Security на всех защищаемых устройствах одной группы администрирования.

Вы можете создать несколько политик для одной группы администрирования и применять их попеременно. Политика, действующая в группе в текущий момент, в Консоли администрирования имеет *активный* статус.

Информация о применении политики регистрируется в журнале системного аудита Kaspersky Embedded Systems Security. Вы можете просмотреть эту информацию в Консоли программы в узле **Журнал системного аудита**.

В Kaspersky Security Center существует единственный способ применения политик на защищаемых устройствах: *Запретить изменение параметров*. После применения политики Kaspersky Embedded Systems Security использует на защищаемых устройствах значения параметров, для которых в свойствах политики вы установили значок , вместо значений параметров, действующих до применения политики. Kaspersky Embedded Systems Security не применяет значения параметров активной политики, для которых в свойствах политики установлен значок .

Если политика активна, то значения параметров, отмеченные в политике значком , отображаются в Консоли программы, но недоступны для редактирования. Значения остальных параметров (отмеченных в политике значком) доступны для редактирования в Консоли программы.

Параметры, настроенные в активной политике и отмеченные значком , также блокируют изменение параметров в окне **Свойства: <Имя защищаемого устройства>** Kaspersky Security Center для отдельного защищаемого устройства.

Параметры, настроенные и переданные на защищаемое устройство с помощью активной политики, сохраняются в параметрах локальных задач после прекращения действия активной политики.

Если политика определяет параметры какой-либо из задач постоянной защиты компьютера и эта задача выполняется, параметры, определенные политикой, изменяются сразу после применения политики. Если задача не выполняется, параметры будут применены при ее запуске.

Создание политики

Чтобы создать политику, выполните следующие действия:

1. В главном окне веб-консоли выберите **Устройства** → **Политики и профили**.
2. Нажмите на кнопку **Добавить**.
3. Откроется окно **Новая политика**.

4. В разделе **Выбор программы** выберите Kaspersky Embedded Systems Security и нажмите на кнопку **Далее**.

5. На закладке **Общие** вы можете выполнить следующие действия:

   - Изменить имя политики.

     Имя политики не должно содержать следующие символы: `" * < : > ? \ | .`

   - Выбрать статус политики:

     - **Активный**. После следующей синхронизации политика будет использоваться на компьютере в качестве активной политики.

     - **Неактивный**. Резервная политика. При необходимости можно перевести неактивную политику в активный статус.

     - **Для автономных пользователей**. Эта политика активируется, когда компьютер покидает периметр сети организации.

   - Настроить наследование параметров:

     - **Наследовать параметры родительской политики**. Если включен этот переключатель, значения параметров политики наследуются из политики верхнего уровня. Параметры политики недоступны для изменения, если для родительской политики установлен .

     - **Принудительное наследование параметров в дочерних политиках**. Если переключатель включен, значения параметров политики распространяются на дочерние политики. В параметрах дочерней политики автоматически устанавливается флажок **Наследовать параметры родительской политики**. Параметры дочерней политики наследуются из родительской политики, за исключением параметров, отмеченных . Параметры дочерней политики недоступны для изменения, если для родительской политики установлен .

6. На закладке **Параметры программы** настройте параметры политики в соответствии с вашими требованиями.

7. Нажмите на кнопку **Сохранить**.

Созданная политика отобразится в списке политик на закладке **Политики и профили** выбранной группы администрирования. В окне **<Имя политики>** вы можете настроить другие параметры, задачи и функции Kaspersky Embedded Systems Security.

Разделы параметров политики Kaspersky Embedded Systems Security

Общие

В разделе **Общие** вы можете настроить следующие параметры политики:

- указать состояние политики;

- настроить наследование параметров для родительских и дочерних политик.

Настройка событий

В разделе **Настройка событий** вы можете настроить параметры для следующих категорий событий:

- *Критическое событие*
- *Отказ функционирования*
- *Предупреждение*
- *Информационное сообщение*
  По кнопке **Свойства** вы можете настроить следующие параметры для выбранных событий:
- указать место и срок хранения информации о зарегистрированных событиях;
- выбрать способ уведомления о зарегистрированных событиях.

Параметры программы

Параметры в разделе Параметры программы

Раздел	Параметры
Масштабируемость и интерфейс	В подразделе **Масштабируемость и интерфейс** по кнопке **Параметры** вы можете настроить следующие параметры: • выбрать автоматическую или ручную настройку параметров масштабирования; • настроить параметры отображения значка программы.
Безопасность	В подразделе **Безопасность** по кнопке **Параметры** вы можете настроить следующие параметры: • настроить параметры запуска задачи; • указать действия программы при переходе защищаемого устройства на источник бесперебойного питания; • включить или выключить защиту функций программы паролем.
Параметры соединения	В подразделе **Параметры соединения** по кнопке **Параметры** вы можете настроить следующие параметры прокси-сервера для соединения с серверами обновлений, серверами активации и KSN: • указать параметры использования прокси-сервера; • указать параметры аутентификации на прокси-сервере.
Запуск системных задач	В подразделе **Запуск системных задач** по кнопке **Параметры** можно разрешить или запретить запуск следующих системных задач по расписанию, настроенному на защищаемых устройствах: • задачи проверки по требованию; • задачи обновления и копирования обновлений.

Дополнительные возможности

Параметры в разделе Дополнительные возможности

Раздел	Параметры
Доверенная зона	В подразделе **Доверенная зона** по кнопке **Параметры** вы можете настроить следующие параметры применения доверенной зоны: • сформировать список исключений доверенной зоны; • включить или выключить проверку операций резервного копирования файлов; • сформировать список доверенных процессов.
Проверка съемных дисков	В подразделе **Проверка съемных дисков** по кнопке **Параметры** вы можете настроить параметры проверки съемных дисков.
Права пользователей на управление программой	В подразделе **Права пользователей на управление программой** вы можете настроить параметры доступа пользователей и групп пользователей на управление Kaspersky Embedded Systems Security.
Права пользователей на управление службой Kaspersky Security	В подразделе **Права пользователей на управление службой Kaspersky Security** вы можете настроить параметры доступа пользователей и групп пользователей к управлению службой Kaspersky Security.
Хранилища	В подразделе **Хранилища** по кнопке **Параметры** вы можете настроить следующие параметры карантина, резервного хранилища и хранилища заблокированных узлов: • указать путь к папке, в которую вы хотите помещать объекты на карантине или в резервном хранилище; • настроить максимальный размер резервного хранилища и карантина, а также указать порог доступного пространства; • указать путь к папке, в которую вы хотите помещать объекты, восстановленные из резервного хранилища или карантина; • настроить передачу информации об объектах резервного хранилища и карантина на Сервер администрирования. • настроить продолжительность блокировки узлов.

Постоянная защита компьютера

Параметры в разделе Постоянная защита сервера

Раздел	Параметры
Постоянная защита файлов	В подразделе **Постоянная защита файлов** по кнопке **Параметры** вы можете настроить следующие параметры задачи: • указать режим защиты объектов; • настроить применение эвристического анализатора;

	• настроить применение доверенной зоны; • указать область защиты; • задать уровень безопасности для выбранной области защиты: вы можете выбрать стандартный уровень безопасности или настроить параметры безопасности вручную; • настроить параметры запуска задачи.
Использование KSN	В подразделе **Использование KSN** по кнопке **Параметры** вы можете настроить следующие параметры задачи: • указать действия над объектами, недоверенными в KSN; • настроить передачу данных и использование Kaspersky Security Center в качестве прокси-сервера KSN.
Защита от эксплойтов	В подразделе **Защита от эксплойтов** по кнопке **Параметры** вы можете настроить следующие параметры задачи: • выбрать режим защиты памяти процессов; • указать действия для снижения рисков эксплуатации уязвимостей; • дополнить и изменить список защищаемых процессов.

Контроль активности на компьютерах

Параметры в разделе Контроль активности на компьютерах

Раздел	Параметры
Контроль запуска программ	В подразделе **Контроль запуска программ** по кнопке **Параметры** вы можете настроить следующие параметры задачи: • выбрать режим работы задачи; • настроить параметры контроля повторных запусков программ; • указать область применения правил контроля запуска программ; • настроить использование KSN; • настроить параметры запуска задачи.
Контроль устройств	В подразделе **Контроль устройств** по кнопке **Параметры** вы можете настроить следующие параметры задачи: • выбрать режим работы задачи; • настроить параметры запуска задачи.

Контроль активности в сети

Параметры в разделе Контроль активности в сети

Раздел	Параметры
Управление сетевым экраном	В подразделе **Управление сетевым экраном** по кнопке **Параметры** вы можете настроить следующие параметры задачи: • настроить правила сетевого экрана; • настроить параметры запуска задачи.

Диагностика системы

Параметры в разделе Диагностика системы

Раздел	Параметры
Мониторинг файловых операций	В подразделе **Мониторинг файловых операций** можно настроить контроль изменений в файлах, которые могут указывать на нарушение безопасности на защищаемом устройстве.
Анализ журналов	В подразделе **Анализ журналов** можно настроить контроль целостности защищаемого устройства на основе результатов анализа журнала событий Windows.

Журналы и уведомления

Параметры в разделе Журналы и уведомления

Раздел	Параметры
Журналы выполнения задач	В подразделе **Журналы выполнения задач** по кнопке **Параметры** вы можете настроить следующие параметры: • указать уровень важности регистрируемых событий для выбранных компонентов программы; • указать параметры хранения журналов выполнения задач; • указать параметры интеграции SIEM-системы с Kaspersky Security Center.
Уведомления о событиях	В подразделе **Уведомления о событиях** по кнопке **Параметры** вы можете настроить следующие параметры: • указать параметры уведомления пользователя для событий *Обнаружен объект*, *Обнаружено и заблокировано недоверенное запоминающее устройство* и *Недоверенный узел в списке*; • указать параметры уведомления администратора для любого выбранного события из списка событий в разделе **Настройка уведомлений**.
Взаимодействие с Сервером администрирования	В подразделе **Взаимодействие с Сервером администрирования** по кнопке **Параметры** вы можете выбрать типы объектов, информацию о которых Kaspersky Embedded Systems Security будет передавать на Сервер администрирования.

История ревизий

В разделе **История ревизий** вы можете управлять ревизиями: сравнивать с текущей ревизией или другой политикой, добавлять описания ревизий, сохранять ревизии в файл или выполнить откат.

Создание и настройка задач в Kaspersky Security Center

Этот раздел содержит информацию о задачах Kaspersky Embedded Systems Security, их создании, настройке параметров выполнения, запуске и остановке.

О создании задач в Kaspersky Security Center Web Console

Вы можете создавать групповые задачи для групп администрирования и для наборов защищаемых устройств. Вы можете создавать задачи следующих типов:

- Активация программы
- Копирование обновлений
- Обновление баз программы
- Обновление модулей программы
- Откат обновления баз программы
- Проверка по требованию
- Проверка целостности программы
- Мониторинг целостности файлов на основе эталона
- Формирование правил контроля запуска программ
- Формирование правил контроля устройств

Вы можете создать локальные и групповые задачи следующими способами:

- для отдельного защищаемого устройства: в окне **Свойства <Имя защищаемого устройства>** в разделе **Задачи**;
- для группы администрирования: в панели результатов узла выбранной группы защищаемых устройств на закладке **Задачи**;
- для набора защищаемых устройств: в панели результатов узла **Выборки устройств**.

С помощью политик можно отключить расписания локальных системных задач Обновление и Проверка по требованию на всех защищаемых устройствах одной группы администрирования.

Общая информация о задачах в Kaspersky Security Center приведена в *Справке Kaspersky Security Center*.

Создание задачи в Kaspersky Security Center Web Console

Чтобы создать новую задачу в Консоли администрирования Kaspersky Security Center, выполните следующие действия:

1. Запустите мастер создания задачи одним из следующих способов:

   - Для создания локальной задачи:

     a. В главном окне веб-консоли выберите **Устройства** → **Управляемые устройства**.

     b. Перейдите на закладку **Группы** и выберите группу администрирования, к которой принадлежит защищаемое устройство.

     c. Выберите название защищаемого устройства.

     d. В открывшемся окне **<Имя устройства>** выберите закладку **Задачи**.

     e. Нажмите на кнопку **Добавить**.

   - Для создания групповой задачи:

     a. В главном окне веб-консоли выберите **Устройства** → **Управляемые устройства**.

     b. Перейдите на закладку **Группы** и выберите группу администрирования, для которой требуется создать задачу.

     c. Нажмите на кнопку **Добавить**.

   - Чтобы создать задачу для произвольного набора защищаемых устройств, выполните следующие действия:

     a. В главном окне веб-консоли выберите **Устройства** → **Выборки устройств**.

     b. Выберите выборку устройств, для которой требуется создать задачу.

     c. Нажмите на кнопку **Запустить**.

     d. В окне **Результаты выборки** выберите устройства, для которых требуется создать задачу.

     e. Нажмите на кнопку **Создать задачу**.

   Откроется окно мастера создания задачи.

2. В раскрывающемся списке **Программы** выберите **Kaspersky Embedded Systems Security**.

3. В раскрывающемся списке **Тип задачи** выберите тип создаваемой задачи.

4. Если вы выбрали любой тип задачи, кроме Откат обновления баз программы, Проверка целостности программы и Активация программы, откроется окно параметров. В зависимости от типа задачи параметры могут различаться.

   - Создайте задачу проверки по требованию.

- Для создания задачи обновления настройте параметры задачи в соответствии с вашими требованиями:

  a. Выберите источник обновлений в разделе **обновления баз программы**.

  b. В окне **Настройка параметров соединения** настройте параметры прокси-сервера.

- После создания задачи Обновление модулей программы настройте параметры обновления требуемых программных модулей в окне **Обновление модулей программы**:

  a. Выберите либо копирование и установку критических обновлений модулей программы, либо только проверку их наличия, без установки.

  b. Если вы выбрали **Копировать и устанавливать критические обновления модулей программы**, для применения установленных программных модулей может потребоваться перезагрузка защищаемого устройства. Чтобы программа Kaspersky Embedded Systems Security автоматически запускала перезагрузку защищаемого устройства после завершения задачи, установите флажок **Разрешать перезагрузку операционной системы**.

  c. Если вы хотите получать информацию о выходе обновлений модулей Kaspersky Embedded Systems Security, установите флажок **Получать информацию о доступных плановых обновлениях модулей программы**.

  "Лаборатория Касперского" не публикует плановые пакеты обновлений на серверах обновлений для автоматической установки; вы можете загружать их с веб-сайта "Лаборатории Касперского". Можно настроить уведомление администратора о событии **Доступно плановое обновление модулей программы**. Оно будет включать адрес нашего веб-сайта, на котором можно загрузить запланированные обновления.

- Для создания задачи Копирование обновлений укажите состав обновлений и папку, в которую будут сохранены обновления, в окне **Копирование обновлений**.

- Для создания задачи Активация программы:

  a. В окне **Не применена политика Kaspersky Security Center** укажите файл ключа, с помощью которого вы хотите активировать программу.

  b. Установите флажок **Использовать в качестве дополнительного ключа**, если вы хотите создать задачу для продления срока действия лицензии.

- Создайте задачу Формирование правил контроля запуска программ и настройте ее параметры.

- Создайте задачу Формирование правил контроля устройств и настройте ее параметры.

5. Нажмите на кнопку **Далее**.

6. Если задача создана для набора защищаемых устройств, выберите сеть (группу) защищаемых устройств, на которых она будет выполняться.

7. Нажмите на кнопку **Далее**.

8. В окне **Завершение создания задачи** установите флажок **Перейти к параметрам задачи после создания**, чтобы настроить параметры задачи.

9. Нажмите на кнопку **Готово**.

Созданная задача отобразится в списке **Задачи**.

Настройка групповых задач в Kaspersky Security Center

Чтобы настроить групповую задачу для нескольких защищаемых устройств, выполните следующие действия:

1. В главном окне веб-консоли выберите **Устройства** → **Задачи**.
2. Щелкните по названию задачи в списке задач Kaspersky Security Center.

   Откроется окно **<Название задачи>**.
3. В зависимости от типа настраиваемой задачи выполните одно из следующих действий:

   - Если вы настраиваете задачу проверки по требованию:

     a. В разделе **Область проверки** настройте область проверки.

     b. В разделе **Параметры** настройте приоритет задачи и интеграцию с другими компонентами программы.

   - Для настройки задачи обновления укажите параметры задачи в соответствии с вашими требованиями:

     a. В разделе **Источник обновлений** настройте параметры источника обновлений и прокси-сервера.

     b. В разделе **Уведомления** настройте параметры оптимизации дисковой подсистемы.

   - Чтобы настроить задачу Обновление модулей программы, в разделе **Дополнительные параметры** выберите действие, которое требуется выполнить: копировать и устанавливать критические обновления программных модулей или только проверять их наличие.

   - Чтобы настроить задачу Копирование обновлений, в разделе **Параметры копирования обновлений** укажите состав обновлений и папку назначения.

   - Чтобы настроить задачу Активация программы, примените файл ключа, с помощью которого вы хотите активировать программу. Установите флажок **Использовать в качестве дополнительного ключа**, если вы хотите добавить код активации или файл ключа для продления срока действия лицензии.

   - Чтобы настроить автоматическое формирование разрешающих правил контроля устройств, укажите параметры, на основе которых будет сформирован список разрешающих правил.
4. В разделе **Расписание** настройте параметры расписания задачи (вы можете настраивать расписание всех задач, кроме задачи Откат обновления баз программы).
5. На закладке **Параметры** в разделе **Учетная запись** укажите учетную запись, с правами которой будет выполняться задача. Подробная информация о настройке параметров в этом разделе приведена в *Справке Kaspersky Security Center*.
6. Нажмите на кнопку **Сохранить**.

Настроенные параметры групповых задач будут сохранены.

Настройка параметров диагностики сбоев в Kaspersky Security Center

Если в работе Kaspersky Embedded Systems Security возникла проблема (например, аварийное завершение Kaspersky Embedded Systems Security) и вы хотите диагностировать ее, вы можете включить создание файлов трассировки и файла дампа процессов Kaspersky Embedded Systems Security и отправить эти файлы на анализ в Службу технической поддержки "Лаборатории Касперского".

Kaspersky Embedded Systems Security не отправляет файлы трассировки и файлы дампов автоматически. Диагностические данные могут быть отправлены только пользователем с соответствующими правами.

Kaspersky Embedded Systems Security записывает информацию в файлы трассировки и файлы дампов в незашифрованном виде. Папка, в которую сохраняются файлы, выбирается пользователем и контролируется параметрами операционной системы и Kaspersky Embedded Systems Security. Можно настроить права доступа и разрешить доступ к журналам, файлам трассировки и файлам дампов только для выбранных пользователей.

Чтобы настроить параметры диагностики сбоев в Kaspersky Security Center, выполните следующие действия:

1. В Консоли администрирования Kaspersky Security Center откройте окно **Параметры программы**.
2. Откройте раздел **Диагностика сбоев** и выполните следующие действия:
   - Если вы хотите записывать отладочную информацию в файл, установите флажок **Записывать отладочную информацию в файл трассировки**.
     - В поле ниже укажите папку, в которую Kaspersky Embedded Systems Security будет сохранять файлы трассировки.
     - Настройте уровень детализации отладочной информации.
     - Укажите максимальный размер файлов трассировки.
     - Укажите максимальное количество файлов в одном журнале трассировки.

       Kaspersky Embedded Systems Security создает не более указанного максимального количества файлов трассировки для каждого отлаживаемого компонента.

     - Укажите отлаживаемые компоненты. Коды компонентов требуется вводить через запятую и с соблюдением регистра (см. таблицу ниже).

Коды подсистем Kaspersky Embedded Systems Security

Код подсистемы	Название подсистемы
*	Все компоненты.
gui	Подсистема пользовательского интерфейса, оснастка Kaspersky Embedded Systems Security в Microsoft Management Console.
ak_conn	Подсистема интеграции с Агентом администрирования Kaspersky Security Center.
bl	Управляющий процесс, реализует задачи управления Kaspersky Embedded Systems Security.
wp	Рабочий процесс; реализует задачи антивирусной защиты.

blgate	Процесс удаленного управления Kaspersky Embedded Systems Security.
ods	Подсистема проверки по требованию.
oas	Подсистема постоянной защиты файлов.
qb	Подсистема карантина и резервного хранилища.
scandll	Вспомогательный модуль антивирусной проверки.
core	Подсистема базовой антивирусной функциональности.
avscan	Подсистема антивирусной обработки.
avserv	Подсистема управления антивирусным ядром.
prague	Подсистема базовой функциональности.
updater	Подсистема обновления баз и модулей программы.
snmp	Подсистема поддержки SNMP протокола.
perfcount	Подсистема счетчиков производительности.

Параметры трассировки оснастки Kaspersky Embedded Systems Security (gui) и Плагина управления для Kaspersky Security Center (ak_conn) применяются после перезапуска этих компонентов. Параметры трассировки подсистемы поддержки SNMP-протокола (snmp) применяются после перезапуска службы SNMP. Параметры трассировки подсистемы счетчиков производительности (perfcount) применяются после перезапуска всех процессов, использующих счетчики производительности. Параметры трассировки остальных подсистем Kaspersky Embedded Systems Security применяются сразу после сохранения параметров диагностики сбоев.

По умолчанию Kaspersky Embedded Systems Security сохраняет отладочную информацию о работе всех компонентов Kaspersky Embedded Systems Security.

Поле ввода доступно, если установлен флажок **Записывать отладочную информацию в файл трассировки**.

- Если вы хотите, чтобы создавался файл дампа, установите флажок **Создавать во время сбоя файл дампа**.
    - В поле ниже укажите папку, в которую Kaspersky Embedded Systems Security будет сохранять файл дампа.

3. Нажмите на кнопку **OK**.

Настроенные параметры программы будут применены на защищаемом устройстве.

Работа с расписанием задач

Можно настроить расписание запуска задач Kaspersky Embedded Systems Security, а также настроить параметры запуска по расписанию.

Настройка расписания запуска задач

В Консоли программы вы можете настроить расписание запуска локальных системных и пользовательских задач. Расписание запуска групповых задач настраивать нельзя.

Чтобы настроить расписание запуска групповой задачи, выполните следующие действия:

1. В главном окне веб-консоли выберите **Устройства** → **Задачи**.
2. Щелкните по названию задачи в списке задач Kaspersky Security Center.

   Откроется окно **<Название задачи>**.
3. Перейдите в раздел **Параметры программы**.
4. В разделе **Расписание** установите флажок **Запускать задачу по расписанию**.

   Поля с параметрами расписания задачи проверки по требованию и задачи обновления недоступны, если запуск этих задач по расписанию запрещен политикой Kaspersky Security Center.
5. Настройте параметры расписания в соответствии с вашими требованиями. Для этого выполните следующие действия:

   a. в списке **Частота запуска** выберите одно из следующих значений:

   - **Ежечасно**, если вы хотите, чтобы задача запускалась периодически через заданное количество часов, и укажите количество часов в поле **Раз в <количество> часов**.
   - **Ежесуточно**, если вы хотите, чтобы задача запускалась периодически через заданное количество дней, и укажите количество дней в поле **Раз в <количество> дней**.
   - **Еженедельно**, если вы хотите, чтобы задача запускалась периодически через заданное количество недель, и укажите количество недель в поле **Раз в <количество> недель**. Укажите, по каким дням недели будет запускаться задача (по умолчанию задача запускается по понедельникам).
   - **При запуске программы**, если вы хотите, чтобы задача запускалась при каждом запуске Kaspersky Embedded Systems Security.
   - **После обновления баз программы**, если вы хотите, чтобы задача запускалась после каждого обновления баз программы.

   b. В поле **Время запуска** укажите время первого запуска задачи.

   c. В поле **Начать с** укажите дату начала действия расписания.
6. В блоке **Параметры остановки задачи**:

   a. Установите флажок **Длительность** и в полях справа укажите максимальную длительность выполнения задачи (количество часов и минут).

   b. Установите флажок **Приостановить задачу** и в полях справа укажите начальное и конечное значение временного промежутка в пределах суток, в течение которого выполнение задачи будет приостановлено.
7. В блоке **Дополнительные параметры расписания**:

   a. Установите флажок **Отменить расписание с** и укажите дату, начиная с которой расписание перестанет действовать.

   b. Установите флажок **Запускать пропущенные задачи**, чтобы включить запуск пропущенных задач.

c. Установите флажок **Распределять время запуска задач в интервале** и укажите значение параметра в минутах.

8. Нажмите на кнопку **Сохранить**, чтобы сохранить параметры запуска задачи.

Включение и выключение запуска задач по расписанию

Вы можете включать и выключать запуск задач по расписанию как после, так и до настройки параметров расписания.

Чтобы включить или выключить расписание запуска задачи, выполните следующие действия:

1. В главном окне веб-консоли выберите **Устройства** → **Задачи**.
2. Щелкните по названию задачи в списке задач Kaspersky Security Center.

   Откроется окно **<Название задачи>**.
3. Перейдите в раздел **Параметры программы**.
4. Выберите раздел **Расписание**.
5. Выполните одно из следующих действий:

   - Установите флажок **Запускать задачу по расписанию**, если вы хотите включить запуск задачи по расписанию.
   - Снимите флажок **Запускать задачу по расписанию**, если вы хотите выключить запуск задачи по расписанию.

     Настроенные параметры расписания запуска задачи не будут удалены и применятся при следующем включении запуска задачи по расписанию.
6. Нажмите на кнопку **Сохранить**.

Настроенные параметры запуска задачи по расписанию будут сохранены.

Отчеты в Kaspersky Security Center

Отчеты в Kaspersky Security Center содержат информацию о состоянии управляемых устройств. Отчеты формируются на основании информации, хранящейся на Сервере администрирования.

Начиная с Kaspersky Security Center 11, для Kaspersky Embedded Systems Security доступны следующие типы отчетов:

- отчет о статусе компонентов;
- отчет о запрещенных запусках;
- отчет о тестовых запрещенных запусках.

Подробную информацию о настройке и работе с отчетами Kaspersky Security Center см. в *Справке Kaspersky Security Center*.

Отчет о статусе компонентов Kaspersky Embedded Systems Security

Вы можете контролировать состояние защиты всех устройств в сети и получать организованное представление о наборе компонентов на каждом устройстве.

В отчете для каждого компонента может отображаться одно из следующих состояний: *Работает*, *Приостановлен*, *Остановлен*, *Неисправен*, *Не установлен*, *Запускается*.

Состояние *Не установлен* относится к компонентам программы, а не к самой программе. Если программа не установлена, Kaspersky Security Center Web Console присваивает статус N/A (недоступно).

Можно создавать выборки компонентов и использовать фильтры, чтобы отображать сетевые устройства с определенным набором компонентов и их состояниями.

Подробную информацию о создании и использовании выборок см. в *Справке Kaspersky Security Center*.

Чтобы просмотреть статусы компонентов в параметрах программы, выполните следующие действия:

1. В главном окне веб-консоли выберите **Устройства** → **Управляемые устройства**.
2. Выберите название защищаемого устройства.
3. На закладке **Общие** выберите раздел **Компоненты**.
4. Ознакомьтесь с таблицей состояния компонентов.

   Информация о статусе компонента Защита от эксплойтов недоступна в этой таблице.

Чтобы просмотреть стандартный отчет Kaspersky Security Center Web Console, выполните следующие действия:

1. Выберите **Мониторинг и отчетность** → **Отчеты**.
2. В списке выберите **Отчет о статусе компонентов программы** и нажмите на кнопку **Показать отчет**.

   Будет сформирован отчет.
3. Ознакомьтесь со следующими элементами отчета:

   - диаграмма;
   - итоговая таблица с компонентами и суммарным количеством устройств в сети, на которых установлен каждый из компонентов, а также группы, к которым они принадлежат;
   - детальная таблица, показывающая статус, версию, устройство и группу компонента.

Отчеты о запрещенных программах в активном и в тестовом режимах

По результатам выполнения задачи Контроль запуска программ можно сформировать два типа отчетов: отчет о запрещенных программах (если задача запущена в активном режиме) и отчет о запрещенных программах в тестовом режиме (если задача запущена в режиме Только статистика). В этих отчетах приведена информация о заблокированных программах на защищаемых устройствах сети. Каждый отчет формируется для всех групп администрирования и содержит данные обо всех программах "Лаборатории Касперского", установленных на защищаемых устройствах.

Чтобы просмотреть отчет о запрещенных программах в режиме Только статистика, выполните следующие действия:

1. Запустите задачу Контроль запуска программ в режиме Только статистика.
2. Выберите **Мониторинг и отчетность** → **Отчеты**.
3. В списке выберите **Отчет о запрещенных программах в тестовом режиме** и нажмите на кнопку **Показать отчет**.

   Будет сформирован отчет.
4. Ознакомьтесь со следующими элементами отчета:

   - диаграмма, показывающая десять программ с самым большим количеством заблокированных запусков;
   - итоговая таблица блокировок программ, содержащая имя исполняемого файла, причину и время блокировки, а также количество устройств, на которых произошла блокировка программ;
   - детальная таблица, показывающая данные устройства, путь к файлу и причину блокировки.

Чтобы просмотреть отчет о запрещенных программах в активном режиме, выполните следующие действия:

1. Запустите задачу Контроль запуска программ в режиме Активный.
2. Выберите **Мониторинг и отчетность** → **Отчеты**.
3. В списке выберите **Отчет о запрещенных программах в тестовом режиме** и нажмите на кнопку **Показать отчет**.

   Будет сформирован отчет.

Отчет содержит те же разделы данных, что и отчет о запрещенных программах в тестовом режиме.

Диагностическое окно

В этом разделе описано использование диагностического окна для просмотра статуса или текущей активности защищаемого устройства и настройка записи файлов дампов и файлов трассировки.

О диагностическом окне

Компонент Диагностическое окно (далее также CDI) устанавливается и удаляется вместе с компонентом Значок области уведомлений независимо от Консоли программы и может быть использован, даже если Консоль программы не установлена на защищаемом устройстве. Диагностическое окно запускается через значок области уведомлений или путем запуска файла kavfsmui.exe из папки программы на защищаемом устройстве.

В диагностическом окне можно выполнять следующие действия:

- просматривать информацию об общем статусе программы;
- просматривать произошедшие инциденты безопасности;
- просматривать текущую активность на защищаемом устройстве;
- запускать и останавливать запись файлов дампов и файлов трассировки;
- открывать Консоль программы;
- открывать окно **О программе** со списком установленных обновлений и доступных исправлений.

Вы можете просматривать Диагностическое окно, даже если доступ к функциям Kaspersky Embedded Systems Security защищен паролем. Введение пароля не требуется.

Диагностическое окно невозможно настроить через Kaspersky Security Center.

Просмотр состояния Kaspersky Embedded Systems Security с помощью диагностического окна

Чтобы открыть диагностическое окно, выполните следующие действия:

1. По правой клавише мыши откройте контекстное меню значка области уведомлений в панели задач.
2. Выберите пункт **Открыть Диагностическое окно**.

   Откроется **Диагностическое окно**.

На закладке **Статус защиты** можно просмотреть текущий статус ключа, а также статус задач постоянной защиты компьютера и задач обновления. Для уведомления о состояниях защиты используется цветовая индикация (см. таблицу ниже).

Статус защиты в диагностическом окне

Раздел	Состояние

Статус постоянной защиты	Панель *зеленого* цвета отображается при любом из следующих сценариев (при выполнении любого из условий):
	• Рекомендуемая конфигурация:
	  • Задача Постоянная защита файлов запущена с параметрами по умолчанию.
	  • Задача Контроль запуска программ запущена в режиме **Активный** с параметрами по умолчанию.
	• Приемлемая конфигурация:
	  • Задача Постоянная защита файлов настроена пользователем.
	  • Параметры задачи Контроль запуска программ изменены.

	Панель *желтого* цвета отображается, если выполнено одно или несколько из следующих условий: • Задача Постоянная защита файлов приостановлена (пользователем или согласно расписанию). • Задача Контроль запуска программ запущена в режиме **Только статистика**. • Защита от эксплойтов и задача Контроль запуска программ запущены в режиме **Только статистика**.
	Панель *красного* цвета отображается, если выполнены оба условия: • Компонент Постоянная защита файлов не установлен или задача остановлена / приостановлена. • Компонент Контроль запуска программ не установлен или задача запущена в режиме **Только статистика**.
Лицензирование	Панель *зеленого* цвета отображается при действующей лицензии.
	Панель *желтого* цвета отображается, если возникло одно из следующих событий: • *Выполняется проверка статуса лицензии.* • *До истечения срока действия лицензии остается 14 дней и не добавлен дополнительный ключ или код активации.* • *Добавленный ключ помещен в черный список и будет заблокирован.*
	Панель *красного* цвета отображается, если возникло одно из следующих событий: • *Программа не активирована* • *Срок действия лицензии истек* • *Нарушено Лицензионное соглашение* • *Ключ помещен в черный список*

Обновление	Панель *зеленого* цвета отображается, если базы программы актуальны.
	Панель *желтого* цвета отображается, если базы программы устарели.
	Панель *красного* цвета отображается, если базы программы сильно устарели.

Просмотр статистики событий безопасности

На закладке **Статистика** отображаются все события безопасности. Статистика каждой задачи защиты отображается в отдельном блоке, где указано количество инцидентов, а также дата и время возникновения последнего инцидента. При регистрации инцидента цвет блока меняется на красный.

Чтобы просмотреть статистику, выполните следующие действия:

1. По правой клавише мыши откройте контекстное меню значка области уведомлений в панели задач.
2. Выберите пункт **Открыть Диагностическое окно**.

   Откроется **Диагностическое окно**.
3. Выберите закладку **Статистика**.
4. Просмотрите инциденты безопасности для задач защиты.

Просмотр текущей активности программы

На этой закладке вы можете просматривать статус текущих задач и процессов программы, а также оперативно получать сообщения о происходящих критических событиях.

Для отображения статуса активности программы используется цветовая индикация:

- В разделе **Задачи**:
  - *Зеленый цвет*. Не выполнены условия, при которых требовалась бы индикация красным цветом.
  - *Желтый цвет*. Проверка важных областей не проводилась давно.
  - *Красный цвет*. Выполнено как минимум одно из следующих условий:
    - Ни одна задача не запущена и расписание запуска не настроено ни для одной задачи.
    - Ошибки запуска программы зарегистрированы как критические события.
- В разделе **Kaspersky Security Network**:
  - *Зеленый цвет*. Задача Использование KSN запущена.
  - *Желтый цвет*. Положение о KSN принято, но задача не запущена.

Чтобы просмотреть текущую активность программы на защищаемом устройстве, выполните следующие действия:

1. По правой клавише мыши откройте контекстное меню значка области уведомлений в панели задач.
2. Выберите пункт **Открыть Диагностическое окно**.

   Откроется **Диагностическое окно**.
3. Выберите закладку **Текущая активность программы**.
4. В разделе **Задачи** ознакомьтесь со следующей информацией:
   - **Проверка важных областей давно не выполнялась**

     Это поле отображается, только если программа возвращает соответствующее предупреждение о проверке важных областей.
   - **Выполняется сейчас**
   - **Завершены с ошибкой**
   - **Следующий запуск определен по расписанию**
5. В разделе **Kaspersky Security Network** ознакомьтесь со следующей информацией:
   - **Включено с запросами файловой репутации** или **Не используется**
   - Включено с запросами файловой репутации, включена отправка статистики KSN.

     Программа отправляет данные о вредоносных программах, в том числе мошеннических, обнаруженных в ходе выполнения задачи Постоянная защита файлов и задач проверки по требованию, а также отладочную информацию о сбоях при проверке.

     Поле отображается, если флажок **Разрешить отправку статистики Kaspersky Security Network** установлен в параметрах задачи Использование KSN.
6. В разделе **Интеграция с Kaspersky Security Center** ознакомьтесь со следующей информацией:
   - **Разрешено локальное управление**
   - **Наложена политика: <Имя Сервера администрирования>**

Настройка записи файлов дампов и файлов трассировки

В диагностическом окне можно настроить запись файлов дампов и файлов трассировки.

Вы можете также настроить диагностику сбоев в Консоли программы.

Чтобы запустить запись файлов дампов и файлов трассировки, выполните следующие действия:

1. По правой клавише мыши откройте контекстное меню значка области уведомлений в панели задач.
2. Выберите пункт **Открыть Диагностическое окно**.

Откроется **Диагностическое окно**.

3. Выберите закладку **Диагностика сбоев**.

4. Если требуется, настройте следующие параметры трассировки:

   a. Установите флажок **Записывать отладочную информацию в файл трассировки в указанной папке**.

   b. Нажмите на кнопку **Обзор** и укажите папку, в которую Kaspersky Embedded Systems Security будет сохранять файлы трассировки.

      Трассировка будет включена для всех компонентов с параметрами по умолчанию: с уровнем детализации *Отладка* и максимальным размером файла журнала – 50 МБ.

5. Если требуется, настройте следующие параметры записи файлов дампов:

   a. Установите флажок **Создавать файл дампа во время сбоя в указанной папке**.

   b. Нажмите на кнопку **Обзор** и укажите папку, в которую Kaspersky Embedded Systems Security будет сохранять файл дампа.

6. Нажмите на кнопку **Применить**.

   Новая конфигурация будет применена.

Обновление баз и модулей Kaspersky Embedded Systems Security

Этот раздел содержит информацию о задачах обновления баз и модулей Kaspersky Embedded Systems Security, копировании обновлений и откате обновлений баз Kaspersky Embedded Systems Security, а также инструкции по настройке задач обновления баз и модулей программы.

О задачах обновления

В Kaspersky Embedded Systems Security предусмотрено четыре задачи обновления системы: Обновление баз программы, Обновление модулей программы, Копирование обновлений и Откат обновления баз программы.

По умолчанию Kaspersky Embedded Systems Security соединяется с источником обновлений – одним из серверов обновлений "Лаборатории Касперского" – каждый час. Вы можете настраивать все задачи обновления, кроме задачи Откат обновления баз программы. После того как вы измените параметры задачи, Kaspersky Embedded Systems Security применит их новые значения при следующем запуске задачи.

Вы не можете приостанавливать и возобновлять задачи обновления.

Обновление баз программы

По умолчанию Kaspersky Embedded Systems Security копирует базы из источника обновлений на устройство и сразу переходит к их использованию в выполняющейся задаче Постоянная защита компьютера. Задачи проверки по требованию переходят к использованию обновленных баз программы при последующем их запуске.

По умолчанию Kaspersky Embedded Systems Security запускает задачу Обновление баз программы каждый час.

Обновление модулей программы

По умолчанию Kaspersky Embedded Systems Security проверяет доступность обновлений модулей программы в источнике обновлений. Для использования установленных программных модулей требуется перезагрузка защищаемого устройства и / или перезапуск Kaspersky Embedded Systems Security.

По умолчанию Kaspersky Embedded Systems Security запускает задачу Обновление модулей программы еженедельно, по пятницам, в 16:00 (время согласно региональным настройкам защищаемого устройства). В ходе выполнения задачи программа проверяет наличие важных и плановых обновлений модулей Kaspersky Embedded Systems Security, не копируя их.

Копирование обновлений

По умолчанию в ходе выполнения задачи Kaspersky Embedded Systems Security загружает файлы обновлений баз программы и сохраняет их в указанную сетевую или локальную папку, не устанавливая их.

По умолчанию задача Копирование обновлений не выполняется.

Откат обновления баз программы

В ходе выполнения задачи Kaspersky Embedded Systems Security возвращается к использованию баз программы с ранее установленными обновлениями.

По умолчанию задача Откат обновления баз программы не выполняется.

Об обновлении модулей программы

"Лаборатория Касперского" может выпускать пакеты обновлений модулей Kaspersky Embedded Systems Security. Пакеты обновлений делятся на *срочные* (или *критические*) и плановые. Срочные пакеты обновлений устраняют уязвимости и ошибки; плановые добавляют новые функции или улучшают существующие.

Срочные (критичные) пакеты обновлений публикуются на серверах обновлений "Лаборатории Касперского". Вы можете настроить их автоматическую установку с помощью задачи Обновление модулей программы. По умолчанию Kaspersky Embedded Systems Security запускает задачу Обновление модулей программы еженедельно, по пятницам, в 16:00 (время согласно региональным настройкам защищаемого устройства).

"Лаборатория Касперского" не публикует плановые пакеты обновлений на серверах обновлений для автоматического обновления; вы можете загружать их с веб-сайта "Лаборатории Касперского". Вы можете получать информацию о выходе плановых обновлений Kaspersky Embedded Systems Security с помощью задачи Обновление модулей программы.

Вы можете загружать срочные обновления из интернета на каждое защищаемое устройство или использовать одно защищаемое устройство в качестве посредника, копируя на него обновления без установки, а затем распределяя их на защищаемые устройства в сети. Чтобы копировать и сохранять обновления без установки, используйте задачу Копирование обновлений.

Перед тем как установить обновления модулей Kaspersky Embedded Systems Security создает резервные копии модулей, установленных ранее. Если обновление модулей программы прервется или завершится с ошибкой, Kaspersky Embedded Systems Security автоматически вернется к использованию ранее установленных программных модулей. Вы также можете откатить обновление модулей вручную до предыдущих установленных обновлений.

На время установки полученных обновлений служба Kaspersky Security автоматически останавливается, а затем снова запускается.

Об обновлении баз программы

Базы Kaspersky Embedded Systems Security, хранящиеся на защищаемом устройстве, быстро становятся неактуальными. Вирусные аналитики "Лаборатории Касперского" ежедневно обнаруживают сотни новых угроз, создают идентифицирующие их записи и включают их в обновления баз программы. Обновление баз программы представляет собой один или несколько файлов с записями, идентифицирующими угрозы, которые были выявлены за время, истекшее с момента создания предыдущего обновления. Чтобы свести риск заражения устройства к минимуму, рекомендуется регулярно получать обновления баз программы.

По умолчанию, если базы Kaspersky Embedded Systems Security не обновляются в течение недели с момента создания установленных обновлений баз, возникает событие *Базы программы устарели*. Если базы программы не обновляются в течение двух недель, возникает событие *Базы программы сильно устарели*. Информация об актуальности баз отображается в панели результатов узла **Kaspersky Embedded Systems Security** в дереве Консоли программы. Вы можете использовать общие параметры Kaspersky Embedded Systems Security, чтобы указать другое количество дней до возникновения этих событий. Вы можете также настроить уведомления администратора об этих событиях.

Kaspersky Embedded Systems Security загружает обновления баз и модулей программы с FTP- или HTTP-серверов обновлений "Лаборатории Касперского", Сервера администрирования Kaspersky Security Center или из других источников обновлений.

Можно загружать обновления на каждое защищаемое устройство или использовать одно защищаемое устройство в качестве посредника. На него будут копироваться обновления, а затем распространяться на защищаемые устройства. Если вы используете программу Kaspersky Security Center для централизованного управления защитой устройств в организации, можно использовать Сервер администрирования Kaspersky Security Center в качестве посредника для загрузки обновлений.

Вы можете запускать задачи обновления баз программы вручную или по расписанию. По умолчанию Kaspersky Embedded Systems Security запускает задачу Обновление баз программы каждый час.

Если загрузка обновлений прервется или завершится с ошибкой, Kaspersky Embedded Systems Security автоматически вернется к использованию баз с последними установленными обновлениями. В случае повреждения баз Kaspersky Embedded Systems Security можно вручную откатить базы до ранее установленных обновлений.

Схемы обновления баз и модулей антивирусных программ в организации

Выбор источника обновлений в задачах обновления зависит используемой в организации схемы обновления баз и модулей программы.

Вы можете обновлять базы и модули Kaspersky Embedded Systems Security на защищаемых устройствах по следующим схемам:

- Загружать обновления напрямую из интернета на каждое защищаемое устройство (схема 1).
- Загружать обновления из интернета на устройство-посредник и распределять обновления на защищаемые устройства с этого устройства.

  Посредником может служить любое устройство, на котором установлены следующие программы:

  - Kaspersky Embedded Systems Security (схема 2).
  - Сервер администрирования Kaspersky Security Center (схема 3).

Обновление через устройство-посредник позволяет не только снизить интернет-трафик, но и обеспечить дополнительную безопасность защищаемых устройств в сети.

Перечисленные схемы обновлений описаны ниже.

Схема 1. Обновление баз и модулей программы напрямую из интернета

Чтобы настроить получение обновлений Kaspersky Embedded Systems Security напрямую из интернета,

на каждом защищаемом устройстве в параметрах задач Обновление баз программы и Обновление модулей программы укажите серверы обновлений "Лаборатории Касперского" в качестве источника обновлений.

Вы можете указать в качестве источников обновлений другие HTTP- или FTP-серверы, на которых имеется папка обновлений.

Рис. 1. Обновление баз и модулей программы напрямую из интернета

Схема 2. Обновление баз и модулей программы через одно из защищаемых устройств

Чтобы настроить получение обновлений Kaspersky Embedded Systems Security через одно из защищаемых устройств, выполните следующие действия:

1. Скопируйте обновления на выбранное защищаемое устройство. Для этого выполните следующие действия:

   - На выбранном защищаемом устройстве настройте параметры задачи Копирование обновлений:

     a. В качестве источника обновлений укажите серверы обновлений "Лаборатории Касперского".

     b. Укажите папку общего доступа в качестве папки, в которой будут сохранены обновления.

2. Распределите обновления на остальные защищаемые устройства. Для этого выполните следующие действия:

   - На каждом защищаемом устройстве настройте параметры задач Обновление баз программы и Обновление модулей программы (см. рис. ниже).

     a. В качестве источника обновлений укажите папку на диске устройства-посредника, в которую будут загружаться обновления.

Kaspersky Embedded Systems Security будет получать обновления через одно из защищаемых устройств.

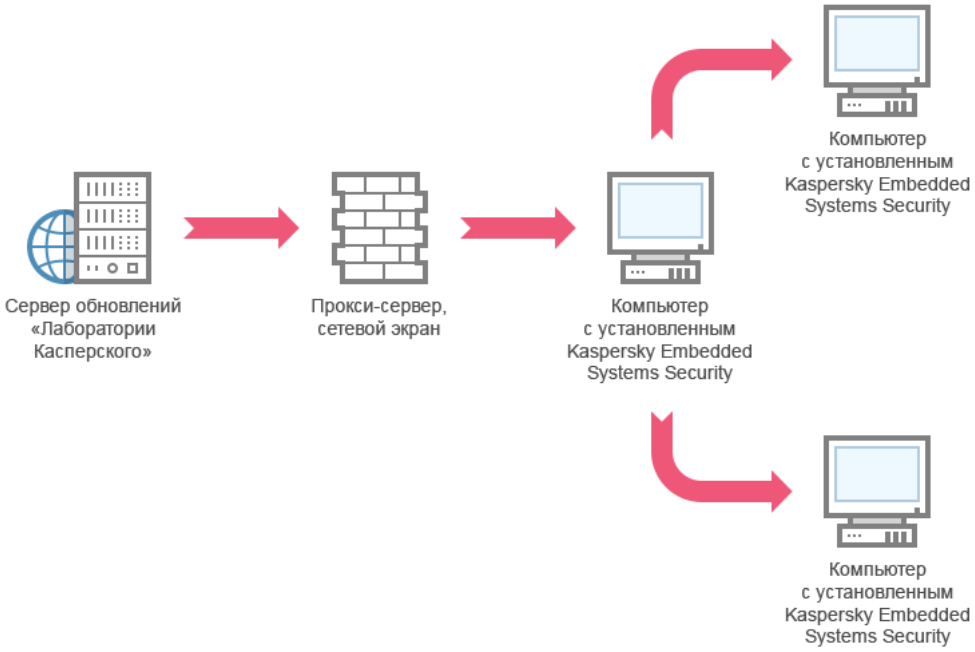

Рис. 2. Обновление баз и модулей программы через одно из защищаемых устройств

Схема 3. Обновление баз и модулей программы через Сервер администрирования Kaspersky Security Center

Если вы используете Kaspersky Security Center для централизованного управления антивирусной защитой устройств, можно загружать обновления с помощью Сервера администрирования Kaspersky Security Center, установленного в локальной сети (см. рис. ниже).

Рис. 3. Обновление баз и модулей программы через Сервер администрирования Kaspersky Security Center

Чтобы настроить получение обновлений Kaspersky Embedded Systems Security через Сервер администрирования Kaspersky Security Center, выполните следующие действия:

1. Загрузите обновления с серверов обновлений "Лаборатории Касперского" на Сервер администрирования Kaspersky Security Center. Для этого выполните следующие действия:

   - Настройте задачу Получение обновлений Сервером администрирования для указанного набора защищаемых устройств:

     a. В качестве источника обновлений укажите серверы обновлений "Лаборатории Касперского".

2. Распределите обновления на защищаемые устройства. Для этого выполните одно из следующих действий:

   - В Kaspersky Security Center настройте групповую задачу обновления антивирусных баз (модулей программы) для распределения обновлений на защищаемые устройства:

     a. В расписании задачи укажите частоту запуска **После получения обновлений Сервером администрирования**.

     Сервер администрирования будет запускать задачу каждый раз, как только он получит обновления (этот способ является рекомендуемым).

     Частоту запуска **После получения обновлений Сервером администрирования** нельзя указать в Консоли программы.

   - Настройте на каждом из защищаемых устройств задачи Обновление баз программы и Обновление модулей программы:

a. В качестве источника обновлений укажите Сервер администрирования Kaspersky Security Center.

b. Если требуется, настройте расписание задачи.

При редких обновлениях антивирусных баз Kaspersky Embedded Systems Security (от одного раза в месяц до одного раза в год) вероятность обнаружения угроз снижается, повышается частота ложных срабатываний компонентов программы.

Kaspersky Embedded Systems Security будет получать обновления через Сервер администрирования Kaspersky Security Center.

Если вы планируете использовать Сервер администрирования Kaspersky Security Center для распределения обновлений, предварительно установите на каждом из защищаемых устройств Агент администрирования – программный компонент, входящий в комплект поставки Kaspersky Security Center. Он обеспечивает взаимодействие между Сервером администрирования и Kaspersky Embedded Systems Security на защищаемом устройстве. Подробная информация об Агенте администрирования и его настройке с помощью Kaspersky Security Center приведена в *Справке Kaspersky Security Center*.

Настройка задач обновления

Этот раздел содержит инструкции по настройке задач обновления Kaspersky Embedded Systems Security.

Настройка параметров работы с источниками обновлений Kaspersky Embedded Systems Security

Для каждой задачи обновления, кроме задачи Откат обновления баз программы, можно указать один или несколько источников обновлений, добавить пользовательские источники обновлений и настроить параметры соединения с указанными источниками обновлений.

После изменения параметров задач обновления новые значения не применяются немедленно в выполняющихся задачах обновления. Настроенные параметры вступят в силу только при последующем запуске задач.

Чтобы указать тип источника обновлений, выполните следующие действия:

1. В дереве Консоли программы разверните узел **Обновление**.
2. Выберите вложенный узел, соответствующий задаче обновления, которую вы хотите настроить.
3. В панели результатов выбранного узла перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи** на закладке **Общие**.
4. В разделе **Источник обновлений** выберите тип источника обновлений Kaspersky Embedded Systems Security:

   - **Сервер администрирования Kaspersky Security Center**
   - **Серверы обновлений "Лаборатории Касперского"**

- **Другие HTTP-, FTP-серверы или сетевые ресурсы**

5. Если требуется, настройте дополнительные параметры для пользовательских источников обновления:

   a. Перейдите по ссылке **Другие HTTP-, FTP-серверы или сетевые ресурсы**.

      1. В открывшемся окне **Серверы обновлений** установите или снимите флажки рядом с пользовательскими источниками обновлений, чтобы начать или прекратить их использование.

      2. Нажмите на кнопку **OK**.

   b. В разделе **Источник обновлений** на закладке **Общие** установите или снимите флажок **Использовать серверы обновлений "Лаборатории Касперского", если серверы, указанные пользователем, недоступны**.

6. В окне **Параметры задачи** выберите закладку **Параметры соединения**, чтобы настроить параметры соединения с источником обновлений:

   - Снимите или установите флажок **Использовать параметры прокси-сервера для соединения с серверами обновлений "Лаборатории Касперского"**.
   - Снимите или установите флажок **Использовать параметры прокси-сервера для соединения с другими серверами**.

   Информация о настройке дополнительных параметров прокси-сервера и параметров аутентификации для доступа к прокси-серверу приведена в разделе Запуск и настройка задачи Обновление баз программы.

7. Нажмите на кнопку **OK**.

Настроенные параметры источника обновлений Kaspersky Embedded Systems Security будут сохранены и применены при последующем запуске задачи.

Вы можете управлять списком пользовательских источников обновлений Kaspersky Embedded Systems Security.

Чтобы отредактировать список пользовательских источников обновлений программы, выполните следующие действия:

1. В дереве Консоли программы разверните узел **Обновление**.
2. Выберите вложенный узел, соответствующий задаче обновления, которую вы хотите настроить.
3. В панели результатов выбранного узла перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи** на закладке **Общие**.
4. Перейдите по ссылке **Другие HTTP-, FTP-серверы или сетевые ресурсы**.

   Откроется окно **Серверы обновлений**.
5. Выполните следующие действия:

   - Чтобы добавить новый пользовательский источник обновления, нажмите на кнопку **Добавить** и в поле ввода укажите адрес папки с файлами обновлений на FTP- или HTTP-сервере. Укажите локальную или сетевую папку в формате UNC (Universal Naming Convention). Нажмите на клавишу **ENTER**.

По умолчанию добавленная папка используется в качестве источника обновлений.

- Чтобы отключить использование пользовательского источника, снимите флажок рядом с источником в списке.
- Чтобы включить использование пользовательского источника, установите флажок рядом с источником в списке.
- Чтобы изменить очередность обращения Kaspersky Embedded Systems Security к пользовательским источникам обновлений, с помощью кнопок **Вверх** и **Вниз** перемещайте выбранный источник к началу или концу списка в зависимости от того, когда он должен использоваться: до или после других источников.
- Чтобы изменить путь к пользовательскому источнику обновлений, выберите источник в списке и нажмите на кнопку **Изменить**, выполните нужные изменения в поле ввода и нажмите на клавишу **ENTER**.
- Чтобы удалить пользовательский источник обновлений, выберите его в списке и нажмите на кнопку **Удалить**.

  Вы не можете удалить единственный пользовательский источник из списка.

6. Нажмите на кнопку **OK**.

Изменения в списке пользовательских источников обновления программы будут сохранены.

Оптимизация дисковой подсистемы при выполнении задачи Обновление баз программы

При выполнении задачи Обновление баз программы Kaspersky Embedded Systems Security размещает файлы обновлений на локальном диске защищаемого устройства. Вы можете снизить нагрузку на дисковую подсистему защищаемого устройства за счет размещения файлов обновлений на виртуальном диске в оперативной памяти при выполнении задачи обновления.

Эта функция доступна для операционных систем Microsoft Windows 7 и выше.

При использовании этой функции во время выполнения задачи Обновление баз программы в операционной системе может появиться дополнительный логический диск. Этот логический диск исчезает из операционной системы после завершения задачи.

Чтобы снизить нагрузку на дисковую подсистему защищаемого устройства при выполнении задачи Обновление баз программы, выполните следующие действия:

1. В дереве Консоли программы разверните узел **Обновление**.
2. Выберите вложенный узел **Обновление баз программы**.
3. В панели результатов узла **Обновление баз программы** перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи** на закладке **Общие**.

4. В разделе **Оптимизация использования дисковой подсистемы** настройте следующие параметры:

   - Снимите или установите флажок **Снизить нагрузку на дисковую подсистему**.

   - В поле **Объем оперативной памяти, используемый для оптимизации (МБ)** укажите объем оперативной памяти в мегабайтах. Операционная система временно выделяет этот объем оперативной памяти для размещения файлов обновлений при выполнении задачи. По умолчанию установлен объем оперативной памяти 512 МБ. Минимально допустимый объем оперативной памяти 400 МБ.

     При запуске задачи Обновление баз программы с включенной функцией оптимизации дисковой подсистемы, может возникнуть одна из следующих ситуаций, в зависимости от того, какой объем оперативной памяти выделен для функции:

     - Если указано слишком маленькое значение, выделенный объем оперативной памяти может оказаться недостаточным для выполнения задачи обновления баз программы (например, при первом обновлении), что приведет к завершению задачи с ошибкой.

       В этом случае рекомендуется выделить больший объем оперативной памяти для функции оптимизации дисковой подсистемы.

     - Если указано слишком большое значение, при запуске задачи обновления баз программы может не получиться создать виртуальный диск требуемого размера в оперативной памяти. В результате функция оптимизации дисковой подсистемы автоматически отключится и задача обновления баз программы будет работать без оптимизации.

       В этом случае рекомендуется выделить меньший объем оперативной памяти для функции оптимизации дисковой подсистемы.

5. Нажмите на кнопку **OK**.

Настроенные параметры будут сохранены и применены при последующем запуске задачи.

Настройка параметров задачи Копирование обновлений

Чтобы настроить параметры задачи Копирование обновлений, выполните следующие действия:

1. В дереве Консоли программы разверните узел **Обновление**.

2. Выберите вложенный узел **Копирование обновлений**.

3. В панели результатов узла **Копирование обновлений** перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи**.

4. На закладках **Общие** и **Параметры соединения** настройте параметры работы с источниками обновлений.

5. На закладке **Общие** в разделе **Параметры копирования обновлений** выполните следующие действия:

   - Укажите условия копирования обновлений программы:

     - **Копировать обновления баз программы**
     - **Копировать критические обновления модулей программы**
     - **Копировать обновления баз программы и критические обновления модулей программы**

- Укажите локальную или сетевую папку, в которую Kaspersky Embedded Systems Security будет копировать полученные обновления.

6. На закладках **Расписание** и **Дополнительно** настройте расписание запуска задачи.
7. На закладке **Запуск с правами** настройте запуск задачи с использованием прав определенной учетной записи.
8. Нажмите на кнопку **OK**.

Настроенные параметры будут сохранены и применены при последующем запуске задачи.

Настройка параметров задачи Обновление модулей программы

Чтобы настроить параметры задачи Обновление модулей программы, выполните следующие действия:

1. В дереве Консоли программы разверните узел **Обновление**.
2. Выберите вложенный узел **Обновление модулей программы**.
3. В панели результатов узла **Обновление модулей программы** перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи**.
4. На закладках **Общие** и **Параметры соединения** настройте параметры работы с источниками обновлений.
5. На закладке **Общие** в разделе **Параметры обновления** настройте параметры обновления модулей программы:
   - **Только проверять наличие доступных критических обновлений модулей программы**
   - **Копировать и устанавливать критические обновления модулей программы**
   - **Разрешать перезагрузку компьютера**
   - **Получать информацию о доступных плановых обновлениях модулей программы**
6. На закладках **Расписание** и **Дополнительно** настройте расписание запуска задачи. По умолчанию Kaspersky Embedded Systems Security запускает задачу Обновление модулей программы еженедельно, по пятницам, в 16:00 (время согласно региональным настройкам защищаемого устройства).
7. На закладке **Запуск с правами** настройте запуск задачи с использованием прав определенной учетной записи.
8. Нажмите на кнопку **OK**.

Настроенные параметры будут сохранены и применены при последующем запуске задачи.

"Лаборатория Касперского" не публикует плановые пакеты обновлений на серверах обновлений для автоматической установки; вы можете загружать их с веб-сайта "Лаборатории Касперского". Вы можете настроить уведомление администратора о событии *Доступны критические и плановые обновления*, в котором будет содержаться адрес веб-страницы, откуда можно загрузить плановые обновления.

Откат обновления баз Kaspersky Embedded Systems Security

Перед применением обновления баз Kaspersky Embedded Systems Security создает резервные копии баз, которые использовались ранее. Если обновление было прервано или завершилось с ошибкой, Kaspersky Embedded Systems Security автоматически возвращается к использованию ранее установленных баз.

Если после обновления баз у вас возникнут проблемы, вы можете откатить базы до предыдущих установленных обновлений, запустив задачу Откат обновления баз программы.

Чтобы запустить задачу Откат обновления баз программы,

в панели результатов узла **Откат обновления баз программы** перейдите по ссылке **Запустить**.

Откат обновления программных модулей

Названия параметров могут отличаться в разных операционных системах Windows.

Перед применением обновления программных модулей Kaspersky Embedded Systems Security создает резервные копии модулей, используемых в текущий момент. Если обновление модулей было прервано или завершилось с ошибкой, Kaspersky Embedded Systems Security автоматически возвращается к использованию модулей с ранее установленными обновлениями.

Чтобы откатить программные модули, используйте функцию Microsoft Windows **Установка и удаление программ**.

Статистика задач обновления

Во время выполнения задачи обновления вы можете просматривать актуальную информацию об объеме данных, загруженных с момента запуска задачи, а также прочую информацию о выполнении задачи.

После завершения или остановки задачи эту информацию можно просмотреть в журнале выполнения задачи.

Чтобы просмотреть статистику задачи обновления, выполните следующие действия:

1. В дереве Консоли программы разверните узел **Обновление**.
2. Выберите вложенный узел, соответствующий задаче, статистику которой вы хотите просмотреть.

   В панели результатов выбранного узла в блоке **Статистика** отобразится статистика задачи.

Если вы просматриваете задачу Обновление баз программы или Копирование обновлений, в разделе **Статистика** отображается объем данных, загруженных Kaspersky Embedded Systems Security на текущий момент (Полученные данные).

Если вы просматриваете задачу Обновление модулей программы, отображается информация, описанная в следующей таблице.

Поле	Описание
Полученные данные	Общий объем полученных данных
Доступно критических обновлений	Количество критических обновлений, доступных для установки
Доступно плановых обновлений	Количество плановых обновлений, доступных для установки
Ошибок применения обновлений	Если значение этого поля отличается от нуля, обновление не было применено. Название обновления, вызвавшего ошибку, можно посмотреть в журнале выполнения задачи.

Изолирование и резервное копирование объектов

Этот раздел содержит информацию о резервном копировании обнаруженных вредоносных объектов перед их лечением или удалением, а также информацию об изолировании возможно зараженных объектов.

Изолирование возможно зараженных объектов. Карантин

Этот раздел содержит информацию об изолировании возможно зараженных объектов, то есть о помещении этих объектов на карантин, и настройке параметров карантина.

Об изолировании возможно зараженных объектов

Kaspersky Embedded Systems Security перемещает объекты, которые признает возможно зараженными, из исходного местоположения в папку *Карантин*. В целях безопасности объекты, помещенные на карантин, хранятся в зашифрованном виде.

Просмотр объектов на карантине

Вы можете просматривать объекты на карантине в узле **Карантин** Консоли программы.

Чтобы просмотреть объекты на карантине, выполните следующие действия:

1. В дереве Консоли программы разверните узел **Хранилища**.
2. Выберите вложенный узел **Карантин**.

Информация об объектах, помещенных на карантин, отобразится в панели результатов выбранного узла.

Чтобы найти нужный объект в списке объектов на карантине,

отсортируйте объекты или отфильтруйте их.

Сортировка объектов на карантине

По умолчанию объекты на карантине отсортированы в таблице по дате помещения на карантин в обратном хронологическом порядке. Чтобы найти нужный объект, можно отсортировать объекты по графам с информацией об объектах. Результат сортировки сохранится, если вы закроете и снова откроете узел **Карантин** или если вы закроете Консоль программы с сохранением в msc-файл и снова откроете ее из этого файла.

Чтобы отсортировать объекты, выполните следующие действия:

1. В дереве Консоли программы разверните узел **Хранилища**.
2. Выберите вложенный узел **Карантин**.

3. В панели результатов узла **Карантин** выберите заголовок графы, по которой вы хотите отсортировать объекты в таблице.

Объекты в таблице писке будут отсортированы по выбранному параметру.

Фильтрация объектов на карантине

Чтобы найти нужный объект на карантине, можно отфильтровать объекты в таблице – отобразить только те объекты, которые удовлетворяют заданным критериям фильтрации (фильтрам). Результат фильтрации сохранится, если вы закроете и снова откроете узел **Карантин** или если вы закроете Консоль программы с сохранением в msc-файл и снова откроете ее из этого файла.

Чтобы задать фильтры, выполните следующие действия:

1. В дереве Консоли программы разверните узел **Хранилища**.

2. Выберите вложенный узел **Карантин**.

3. В контекстном меню узла выберите пункт **Фильтр**.

   Откроется окно **Параметры фильтра**.

4. Чтобы добавить фильтр, выполните следующие действия:

   a. В списке **Название поля** выберите поле, по которому выполняется фильтрация событий.

   b. В списке **Оператор** выберите условие фильтрации. Условия фильтрации в таблице могут различаться в зависимости от значения, выбранного в списке **Название поля**.

   c. В поле **Значение поля** введите или выберите в списке значение фильтра.

   d. Нажмите на кнопку **Добавить**.

   Добавленный фильтр отобразится в списке фильтров в окне **Параметры фильтра**. Повторите шаги a-d для каждого добавляемого фильтра. При работе с фильтрами используйте следующие рекомендации:

   - Чтобы объединить несколько фильтров по логическому "И", выберите вариант **При выполнении всех условий**.

   - Чтобы объединить несколько фильтров по логическому "ИЛИ", выберите вариант **При выполнении любого условия**.

   - Чтобы удалить фильтр, в списке фильтров выберите фильтр, который вы хотите удалить, и нажмите на кнопку **Удалить**.

   - Чтобы изменить фильтр, выберите фильтр в списке в окне **Параметры фильтра**. Отредактируйте требуемые значения в полях **Название поля**, **Оператор** и **Значение поля** и нажмите на кнопку **Заменить**.

5. После добавления всех фильтров нажмите на кнопку **Применить**.

Созданные фильтры будут сохранены.

Чтобы вернуть отображение всех объектов на карантине,

в контекстном меню узла **Карантин** выберите пункт **Снять фильтр**.

Проверка объектов на карантине

По умолчанию после каждого обновления баз Kaspersky Embedded Systems Security выполняет системную задачу Проверка объектов на карантине. Параметры задачи приведены в следующей таблице. Вы не можете изменять параметры задачи Проверка объектов на карантине.

Можно настраивать расписание запуска задачи, запускать ее вручную, а также изменять права учетной записи, под управлением которой запускается задача.

Проверив объекты на карантине после обновления баз, Kaspersky Embedded Systems Security может признать некоторые из них незараженными: статус таких объектов изменится на **Ложное срабатывание**. Другие объекты Kaspersky Embedded Systems Security может признать зараженными и выполнить над ними действия, предусмотренные параметрами задачи Проверка объектов на карантине: лечить или удалять, если лечение невозможно.

Параметры задачи Проверка объектов на карантине

Параметр задачи Проверка объектов на карантине	Значение
Область проверки	Папка карантина
Параметры безопасности	Единые для всей области проверки (значения приводятся в следующей таблице)

Параметры безопасности в задаче Проверка объектов на карантине

Параметр безопасности	Значение
Проверка объектов	Все объекты области проверки
Оптимизация	Выключено
Действие над зараженными и другими обнаруженными объектами	Лечить, удалять, если лечение невозможно
Действие над возможно зараженными объектами	Пропускать
Исключать объекты	Нет
Не обнаруживать	Нет
Останавливать проверку, если она длится более (сек.)	Не задано
Не проверять объекты размером более (МБ)	Не задано
Альтернативные потоки NTFS	Включена
Загрузочные секторы дисков и MBR	Выключено
Использовать технологию iChecker	Выключено
Использовать технологию iSwift	Выключено
Проверять составные объекты	• Архивы* • SFX-архивы* • Упакованные объекты*

	• Вложенные OLE-объекты* * Проверка только новых и измененных файлов выключена.
Проверка подписи Microsoft у файлов	Не выполняется
Использование эвристического анализатора	Включено с уровнем анализа **Глубокий**
Доверенная зона	Не применяется

Восстановление содержимого карантина

Kaspersky Embedded Systems Security помещает возможно зараженные объекты в папку карантина в зашифрованном виде, чтобы предохранить защищаемое устройство от их возможного вредоносного действия.

Вы можете восстановить любой объект с карантина. Это может потребоваться в следующих случаях:

- если после проверки карантина с применением обновленных баз статус объекта изменился на **Ложное срабатывание** или **Вылечен**;
- если вы считаете объект безопасным для защищаемого устройства и хотите его использовать. Чтобы программа Kaspersky Embedded Systems Security не изолировала этот объект при последующих проверках, вы можете исключить объект из обработки в задаче Постоянная защита файлов и в задачах проверки по требованию. Для этого укажите объект в качестве значения параметра безопасности **Исключать файлы** (по имени файла) или **Не обнаруживать** в этих задачах либо добавьте его в Доверенную зону.

При восстановлении объектов можно выбрать, где будет сохранен восстановленный объект: в исходном местоположении (по умолчанию), в специальной папке для восстановленных объектов на защищаемом устройстве, в указанной папке на защищаемом устройстве, на котором установлена Консоль программы, или на другом устройстве в сети.

Можно указать папку для хранения восстановленных объектов на защищаемом устройстве. Вы можете установить для ее проверки специальные параметры безопасности. Путь к этой папке задается параметрами карантина.

Восстановление объектов из карантина может привести к заражению защищаемого устройства.

Вы можете восстановить объект, сохранив его копию в папке карантина, чтобы использовать ее в дальнейшем, например, чтобы еще раз проверить объект после обновления баз.

Если объект, помещенный на карантин, входит в составной объект (например, в архив), Kaspersky Embedded Systems Security не включает его в составной объект при восстановлении. Объект, помещенный на карантин, сохраняется отдельно в выбранную папку.

Вы можете восстановить один или несколько объектов.

Чтобы восстановить объекты с карантина, выполните следующие действия:

1. В дереве Консоли программы разверните узел **Хранилища**.

2. Выберите вложенный узел **Карантин**.

3. В панели результатов узла **Карантин** выполните одно из следующих действий:

   - Чтобы восстановить один объект, в контекстном меню объекта, который вы хотите восстановить, выберите пункт **Восстановить**.

   - чтобы восстановить несколько объектов, выберите нужные объекты, используя клавишу **Ctrl** или клавишу **Shift**, затем откройте контекстное меню одного из выбранных объектов и выберите пункт **Восстановить**.

   Откроется окно **Восстановление объекта**.

4. В окне **Восстановление объекта** для каждого выбранного объекта укажите папку, в которой будет сохранен восстанавливаемый объект.

   Имя объекта отображается в поле **Объект** в верхней части окна. Если вы выбрали несколько объектов, будет отображаться имя первого объекта в списке.

5. Выполните одно из следующих действий:

   - Чтобы восстановить объект в исходное местоположение, выберите пункт **Восстановить в исходную папку**.

   - Чтобы восстановить объект в папку, которую вы задали в качестве папки для восстановления в параметрах, выберите **Восстановить в папку, используемую по умолчанию**.

   - Чтобы сохранить объект в другую папку на защищаемом устройстве, на котором установлена Консоль программы, или в папку общего доступа, выберите **Восстановить в папку на локальном компьютере или сетевом ресурсе**, а затем выберите нужную папку или укажите путь к ней.

6. Чтобы сохранить копию объекта в папке *Карантин* после его восстановления, снимите флажок **Удалить объекты из хранилища после восстановления**.

7. Чтобы применить указанные условия восстановления к остальным выбранным объектам, установите флажок **Применить ко всем выбранным объектам**.

   Все выбранные объекты будут восстановлены и сохранены в указанное местоположение. Если вы выбрали **Восстановить в исходную папку**, каждый объект будет сохранен в свое исходное местоположение; если вы выбрали **Восстановить в папку, используемую по умолчанию** или **Восстановить в папку на локальном компьютере или сетевом ресурсе**, все объекты будут сохранены в одну указанную папку.

8. Нажмите на кнопку **OK**.

   Kaspersky Embedded Systems Security начнет восстанавливать первый из выбранных вами объектов.

9. Если объект с таким именем уже существует в указанном местоположении, откроется окно **Объект с таким именем существует**.

   a. Выберите одно из следующих действий Kaspersky Embedded Systems Security:

      - **Заменить**, чтобы заменить существующий объект на восстанавливаемый объект.

      - **Переименовать**, чтобы сохранить восстанавливаемый объект под другим именем. В поле ввода введите новое имя файла восстанавливаемого объекта и полный путь к нему.

- **Переименовать, добавив суффикс**, чтобы переименовать восстанавливаемый объект, добавив к имени его файла суффикс. Введите суффикс в поле ввода.

b. Если вы выбрали несколько объектов для восстановления, то, чтобы применить выбранное действие, например, **Заменить** или **Переименовать**, к остальным выбранным объектам, установите флажок **Применить ко всем выбранным объектам**. Если вы выбрали **Переименовать**, флажок **Применить ко всем выбранным объектам** будет недоступен.

c. Нажмите на кнопку **OK**.

Файл будет восстановлен. Информация об операции восстановления будет зарегистрирована в журнале системного аудита.

Если вы не установили флажок **Применить ко всем выбранным объектам** в окне **Восстановление объекта**, то окно **Восстановление объекта** откроется снова. В этом окне можно указать местоположение, куда будет восстановлен следующий выбранный объект (см. шаг 4 этой инструкции).

Помещение объектов на карантин

Вы можете вручную помещать файлы на карантин.

Чтобы поместить файл на карантин, выполните следующие действия:

1. В дереве Консоли программы откройте контекстное меню узла **Карантин**.
2. Выберите пункт **Добавить**.
3. В окне **Открыть** укажите файл, который вы хотите поместить на карантин.
4. Нажмите на кнопку **OK**.

Kaspersky Embedded Systems Security поместит указанный файл на карантин.

Удаление объектов с карантина

Согласно параметрам задачи Проверка объектов на карантине, Kaspersky Embedded Systems Security автоматически удаляет из папки карантина объекты, статус которых изменился на *Зараженный или обнаруживаемый* при проверке карантина с использованием обновленных баз, если программа Kaspersky Embedded Systems Security не смогла их вылечить. Kaspersky Embedded Systems Security не удаляет остальные объекты из карантина.

Можно удалять объекты с карантина.

Чтобы удалить объекты с карантина, выполните следующие действия:

1. В дереве Консоли программы разверните узел **Хранилища**.
2. Выберите вложенный узел **Карантин**.
3. Выполните одно из следующих действий:

- Чтобы удалить один объект, в контекстном меню этого объекта выберите пункт **Удалить**.

- Чтобы удалить несколько объектов, выберите нужные объекты в списке, используя клавиши **CTRL** и **SHIFT**, затем откройте контекстное меню любого из выбранных объектов и выберите пункт **Удалить**.

4. В окне подтверждения нажмите на кнопку **Да**, чтобы подтвердить операцию.

Выбранные объекты будут удалены с карантина.

Отправка возможно зараженных объектов на исследование в "Лабораторию Касперского"

Если поведение какого-нибудь файла дает вам основание подозревать в нем наличие угрозы, а Kaspersky Embedded Systems Security признает этот файл незараженным, то, возможно, вы встретились с новой, неизвестной угрозой, описание которой еще не добавлено в базы. Вы можете отправить этот файл на исследование в "Лабораторию Касперского". Вирусные аналитики "Лаборатории Касперского" проанализируют его и, если обнаружат в нем новую угрозу, добавят идентифицирующую ее запись в базы. Возможно, когда вы вновь проверите объект после обновления баз, Kaspersky Embedded Systems Security признает его зараженным и сможет его вылечить. Вы сможете не только сохранить объект, но и предотвратить вирусную эпидемию.

Вы можете отправлять на исследование только файлы с карантина. Файлы, находящиеся на карантине, хранятся в зашифрованном виде и при пересылке не удаляются антивирусной программой, установленной на почтовом сервере.

Нельзя отправлять объекты с карантина на исследование в "Лабораторию Касперского" после окончания срока действия лицензии.

Чтобы отправить файл на исследование в "Лабораторию Касперского", выполните следующие действия:

1. Если файл не находится на карантине, предварительно поместите его на **Карантин**.

2. В узле **Карантин** откройте контекстное меню файла, который вы хотите отправить на исследование в "Лабораторию Касперского", и выберите пункт **Отправить объект на исследование**.

3. В открывшемся окне подтверждения операции нажмите на кнопку **Да**, если действительно хотите отправить выбранный объект на исследование.

4. Если на защищаемом устройстве, на котором установлена Консоль программы, настроен почтовый клиент, будет создано новое сообщение электронной почты. Просмотрите его, а затем нажмите на кнопку **Отправить**.

   Поле **Получатель** содержит адрес электронной почты "Лаборатории Касперского" – newvirus@kaspersky.com. Поле Тема содержит текст "Объект карантина".

   Текст сообщения содержит следующую информацию: "Этот файл будет отправлен на анализ в Лабораторию Касперского". В тело сообщения вы можете включить любую дополнительную информацию о файле: почему он показался вам возможно зараженным или опасным, как он себя ведет или как влияет на систему.

   К сообщению будет приложен архив <имя объекта>.cab. Архив содержит файл <uuid>.klq с зашифрованным объектом, файл <uuid>.txt с информацией об объекте, полученной из Kaspersky Embedded Systems Security, а также файл Sysinfo.txt, который содержит следующую информацию о Kaspersky Embedded Systems Security и операционной системе защищаемого устройства:

   - название и версию операционной системы;

   - название и версию Kaspersky Embedded Systems Security;

- дату выпуска последних установленных обновлений баз программы;
- активный ключ.

Эта информация нужна вирусным аналитикам "Лаборатории Касперского", чтобы быстрее и более эффективно проанализировать файл. Однако если вы не хотите передавать эту информацию, вы можете удалить файл Sysinfo.txt из архива.

Если почтовый клиент не установлен на защищаемом устройстве, на котором установлена Консоль программы, программа предложит сохранить выбранный зашифрованный объект в файл. Этот файл можно переслать в "Лабораторию Касперского" самостоятельно.

Чтобы сохранить зашифрованный объект в файл, выполните следующие действия:

1. В открывшемся окне с приглашением сохранить объект нажмите на кнопку **OK**.
2. Выберите папку на диске защищаемого устройства или сетевую папку, в которую вы хотите сохранить файл с объектом.

Объект будет сохранен в файл формата CAB.

Настройка параметров карантина

Вы можете настраивать параметры карантина. Новые параметры карантина применяются сразу после сохранения.

Чтобы настроить параметры карантина, выполните следующие действия:

1. В дереве Консоли программы разверните узел **Хранилища**.
2. Откройте контекстное меню вложенного узла **Карантин**.
3. Выберите пункт **Свойства**.
4. В окне **Свойства карантина** настройте нужные параметры карантина в соответствии с вашими требованиями:
   - В разделе **Параметры карантина**:
     - **Папка карантина**
     - **Максимальный размер карантина (МБ)**
     - **Порог доступного пространства (МБ)**

     Если объем объектов на карантине превышает значение максимального размера карантина или превышает порог доступного пространства, Kaspersky Embedded Systems Security уведомит вас об этом, не переставая помещать объекты на карантин.

   - В разделе **Параметры восстановления объектов**:
     - **Папка, в которую восстанавливаются объекты**

5. Нажмите на кнопку **OK**.

Настроенные параметры карантина будут сохранены.

Статистика карантина

Вы можете просматривать информацию о количестве объектов на карантине – статистику карантина.

Чтобы просмотреть статистику карантина,

в дереве Консоли программы в контекстном меню узла **Карантин** выберите пункт **Статистика**.

В окне **Статистика карантина** отображается информация о количестве объектов на карантине в текущий момент (см. таблицу ниже):

Поле	Описание
Возможно зараженных объектов	Количество объектов, которые программа Kaspersky Embedded Systems Security признала возможно зараженными.
Текущий размер карантина	Общий объем данных в папке карантина.
Ложных срабатываний	Количество объектов, которым присвоен статус *Ложное срабатывание*, поскольку при проверке карантина с применением обновленных баз они были признаны незараженными.
Вылечено объектов	Количество объектов, которым присвоен статус *Вылечен* после проверки карантина.
Всего объектов	Общее количество объектов на карантине.

Резервное копирование объектов. Резервное хранилище

Этот раздел содержит информацию о резервном копировании обнаруженных вредоносных объектов перед их лечением или удалением, а также инструкции по настройке параметров резервного хранилища.

О резервном копировании объектов перед лечением или удалением

Kaspersky Embedded Systems Security сохраняет зашифрованные копии объектов со статусом *зараженный* в папке *Резервное хранилище* перед тем, как выполнить лечение или удаление этих объектов.

Если объект является частью составного объекта (например, входит в архив), Kaspersky Embedded Systems Security сохраняет составной объект в резервном хранилище полностью. Например, если Kaspersky Embedded Systems Security признает зараженным один из объектов в составе почтовой базы, он сохраняет копию всей почтовой базы.

Если объект, который Kaspersky Embedded Systems Security помещает в резервное хранилище, имеет большой размер, может произойти замедление работы системы и сокращение свободного места на жестком диске.

Можно восстановить файлы из резервного хранилища как в исходную папку, так и в другую папку на защищаемом устройстве или другом устройстве в локальной сети организации. Вы можете восстановить файл из резервного хранилища, если зараженный файл содержал важную информацию, но при лечении этого файла программа Kaspersky Embedded Systems Security не смогла сохранить его целостность, в результате чего информация в нем стала недоступной.

Восстановление файлов из резервного хранилища может привести к заражению защищаемого устройства.

Просмотр объектов в резервном хранилище

Вы можете просматривать объекты в папке резервного хранилища только с помощью узла **Резервное хранилище** Консоли программы. Вы не можете просматривать их с помощью файловых менеджеров Microsoft Windows.

Чтобы просмотреть объекты в резервном хранилище, выполните следующие действия:

1. В дереве Консоли программы разверните узел **Хранилища**.
2. Выберите вложенный узел **Резервное хранилище**.

   Информация об объектах, помещенных в резервное хранилище, отобразится в панели результатов выбранного узла.

Чтобы найти нужный объект в списке объектов в резервном хранилище,

отсортируйте объекты или отфильтруйте их.

Сортировка файлов в резервном хранилище

По умолчанию файлы в резервном хранилище отсортированы по дате их попадания в резервное хранилище в обратном хронологическом порядке. Чтобы найти нужный файл, отсортируйте файлы по содержимому любой графы в панели результатов.

Результат сортировки сохранится, если вы закроете и снова откроете узел **Резервное хранилище** или если вы закроете Консоль программы с сохранением в msc-файл и снова откроете ее из этого файла.

Чтобы отсортировать файлы в резервном хранилище, выполните следующие действия:

1. В дереве Консоли программы разверните узел **Хранилища**.
2. Выберите вложенный узел **Резервное хранилище**.

3. В таблице файлов в узле **Резервное хранилище** выберите заголовок графы, по содержимому которой вы хотите отсортировать объекты.

Файлы в резервном хранилище будут отсортированы по выбранному критерию.

Фильтрация файлов в резервном хранилище

Чтобы найти нужный файл в резервном хранилище, можно отфильтровать файлы – отобразить в узле **Резервное хранилище** только те файлы, которые удовлетворяют заданным условиям фильтрации (фильтрам).

Результат сортировки сохранится, если вы закроете и снова откроете узел **Резервное хранилище** или если вы закроете Консоль программы с сохранением в msc-файл и снова откроете ее из этого файла.

Чтобы отфильтровать файлы в резервном хранилище, выполните следующие действия:

1. В дереве Консоли программы откройте контекстное меню узла **Резервное хранилище** и выберите пункт **Фильтр**.

   Откроется окно **Параметры фильтра**.

2. Чтобы добавить фильтр, выполните следующие действия:

   a. В списке **Название поля** выберите поле, по которому выполняется фильтрация событий.

   b. В списке **Оператор** выберите условие фильтрации. Условия фильтрации в списке могут различаться в зависимости значения, выбранного в поле **Название поля**.

   c. В поле **Значение поля** введите или выберите в списке значение фильтра.

   d. Нажмите на кнопку **Добавить**.

   Добавленный фильтр отобразится в списке фильтров в окне **Параметры фильтра**. Повторите эти действия для каждого добавляемого фильтра. При работе с фильтрами используйте следующие рекомендации:

   - Чтобы объединить несколько фильтров по логическому "И", выберите вариант **При выполнении всех условий**.
   - Чтобы объединить несколько фильтров по логическому "ИЛИ", выберите вариант **При выполнении любого условия**.
   - Чтобы удалить фильтр, в списке фильтров выберите фильтр, который вы хотите удалить, и нажмите на кнопку **Удалить**.
   - Чтобы отредактировать фильтр, выберите его в списке фильтров в окне **Параметры фильтра**, измените требуемые значения в полях **Название поля**, **Оператор** и **Значение поля** и нажмите на кнопку **Заменить**.

   После того как вы добавите все фильтры, нажмите на кнопку **Применить**. В списке отобразятся только файлы, отобранные согласно заданным фильтрам.

Чтобы снова отобразить все файлы в списке файлов в резервном хранилище,

в контекстном меню узла **Резервное хранилище** выберите пункт **Снять фильтр**.

Восстановление файлов из резервного хранилища

Kaspersky Embedded Systems Security хранит файлы в папке резервного хранилища в зашифрованном виде, чтобы предохранить защищаемое устройство от их возможного вредоносного действия.

Вы можете восстанавливать файлы из резервного хранилища.

Вам может потребоваться восстановить файл в следующих случаях:

- если исходный зараженный файл содержал важную информацию и при лечении файла программа Kaspersky Embedded Systems Security не смогла сохранить его целостность, в результате чего информация в файле стала недоступной;

- если вы считаете файл безопасным для защищаемого устройства и хотите его использовать. Чтобы программа Kaspersky Embedded Systems Security не признавала файл зараженным или возможно зараженным при последующих проверках, вы можете исключить его из обработки в задаче Постоянная защита файлов и в задачах проверки по требованию. Для этого укажите файл в качестве значения параметра **Исключать файлы** или **Не обнаруживать** соответствующих задач.

  Восстановление файлов из резервного хранилища может привести к заражению защищаемого устройства.

При восстановлении файла вы можете выбрать, куда он будет сохранен: в исходное местоположение (по умолчанию), в специальную папку для восстановленных объектов на защищаемом устройстве, в указанную папку на защищаемом устройстве, на котором установлена Консоль программы, или на другом устройстве в сети.

Можно указать папку для хранения восстановленных объектов на защищаемом устройстве. Вы можете установить для ее проверки специальные параметры безопасности. Путь к этой папке задается параметрами резервного хранилища.

По умолчанию, когда Kaspersky Embedded Systems Security восстанавливает файл, его копия сохраняется в резервном хранилище. Вы можете удалить копию файла из резервного хранилища после его восстановления.

Чтобы восстановить файлы из резервного хранилища, выполните следующие действия:

1. В дереве Консоли программы разверните узел **Хранилища**.

2. Выберите вложенный узел **Резервное хранилище**.

3. В панели результатов узла **Резервное хранилище** выполните одно из следующих действий:

   - Чтобы восстановить один объект, в контекстном меню объекта, который вы хотите восстановить, выберите пункт **Восстановить**.

   - чтобы восстановить несколько объектов, выберите нужные объекты, используя клавишу **Ctrl** или клавишу **Shift**, затем откройте контекстное меню одного из выбранных объектов и выберите пункт **Восстановить**.

   Откроется окно **Восстановление объекта**.

4. В окне **Восстановление объекта** для каждого выбранного объекта укажите папку, в которой будет сохранен восстанавливаемый объект.

Имя объекта отображается в поле **Объект** в верхней части окна. Если вы выбрали несколько объектов, будет отображаться имя первого объекта в списке.

5. Выполните одно из следующих действий:

   - Чтобы восстановить объект в исходное местоположение, выберите пункт **Восстановить в исходную папку**.
   - Чтобы восстановить объект в папку, которую вы задали в качестве папки для восстановления в параметрах, выберите **Восстановить в папку, используемую по умолчанию**.
   - Чтобы сохранить объект в другую папку на защищаемом устройстве, на котором установлена Консоль программы, или в папку общего доступа, выберите **Восстановить в папку на локальном компьютере или сетевом ресурсе**, а затем выберите нужную папку или укажите путь к ней.

6. Если вы не хотите сохранить копию файла в папке резервного хранилища после его восстановления, установите флажок **Удалить объекты из хранилища после восстановления** (по умолчанию флажок снят).

7. Чтобы применить указанные условия восстановления к остальным выбранным объектам, установите флажок **Применить ко всем выбранным объектам**.

   Все выбранные объекты будут восстановлены и сохранены в указанное местоположение. Если вы выбрали **Восстановить в исходную папку**, каждый объект будет сохранен в свое исходное местоположение; если вы выбрали **Восстановить в папку, используемую по умолчанию** или **Восстановить в папку на локальном компьютере или сетевом ресурсе**, все объекты будут сохранены в одну указанную папку.

8. Нажмите на кнопку **OK**.

   Kaspersky Embedded Systems Security начнет восстанавливать первый из выбранных вами объектов.

9. Если объект с таким именем уже существует в указанном местоположении, откроется окно **Объект с таким именем существует**.

   a. Выберите одно из следующих действий Kaspersky Embedded Systems Security:

      - **Заменить**, чтобы заменить существующий объект на восстанавливаемый объект.
      - **Переименовать**, чтобы сохранить восстанавливаемый объект под другим именем. В поле ввода введите новое имя файла восстанавливаемого объекта и полный путь к нему.
      - **Переименовать, добавив суффикс**, чтобы переименовать восстанавливаемый объект, добавив к имени его файла суффикс. Введите суффикс в поле ввода.

   b. Если вы выбрали несколько объектов для восстановления, то, чтобы применить выбранное действие, например, **Заменить** или **Переименовать**, к остальным выбранным объектам, установите флажок **Применить ко всем выбранным объектам**. Если вы выбрали **Переименовать**, флажок **Применить ко всем выбранным объектам** будет недоступен.

   c. Нажмите на кнопку **OK**.

   Файл будет восстановлен. Информация об операции восстановления будет зарегистрирована в журнале системного аудита.

Если вы не установили флажок **Применить ко всем выбранным объектам** в окне **Восстановление объекта**, то окно **Восстановление объекта** откроется снова. В этом окне можно указать местоположение, куда будет восстановлен следующий выбранный объект (см. шаг 4 этой инструкции).

Удаление файлов из резервного хранилища

Чтобы удалить файлы из резервного хранилища, выполните следующие действия:

1. В дереве Консоли программы разверните узел **Хранилища**.
2. Выберите вложенный узел **Резервное хранилище**.
3. Выполните одно из следующих действий:
   - Чтобы удалить один объект, в контекстном меню этого объекта выберите пункт **Удалить**.
   - Чтобы удалить несколько объектов, выберите нужные объекты в списке, используя клавиши **CTRL** и **SHIFT**, затем откройте контекстное меню любого из выбранных объектов и выберите пункт **Удалить**.
4. В окне подтверждения нажмите на кнопку **Да**, чтобы подтвердить операцию.

Выбранные файлы будут удалены из резервного хранилища.

Настройка параметров резервного хранилища

Чтобы настроить параметры резервного хранилища, выполните следующие действия:

1. В дереве Консоли программы разверните узел **Хранилища**.
2. Откройте контекстное меню вложенного узла **Резервное хранилище**.
3. Выберите пункт **Свойства**.
4. В окне **Свойства резервного хранилища** настройте нужные параметры резервного хранилища в соответствии с вашими требованиями:

   В разделе **Параметры резервного хранилища**:

   - **Папка резервного хранилища**
   - **Максимальный размер резервного хранилища (МБ)**
   - **Порог доступного пространства (МБ)**

     Если объем объектов в резервном хранилище превышает значение максимального размера резервного хранилища или превышает порог доступного пространства, Kaspersky Embedded Systems Security уведомит вас об этом, не переставая помещать объекты в резервное хранилище.

   В разделе **Параметры восстановления объектов**:

   - **Папка, в которую восстанавливаются объекты**
5. Нажмите на кнопку **OK**.

Настроенные параметры резервного хранилища будут сохранены.

Статистика резервного хранилища

Можно просматривать информацию о текущем состоянии резервного хранилища – статистику резервного хранилища.

Чтобы просмотреть статистику резервного хранилища,

в дереве Консоли программы откройте контекстное меню узла **Резервное хранилище** и выберите пункт **Статистика**. Откроется окно **Статистика резервного хранилища**.

В окне **Статистика резервного хранилища** отображается информация о текущем состоянии резервного хранилища (см. таблицу ниже).

Информация о текущем состоянии резервного хранилища

Поле	Описание
Текущий размер резервного хранилища	Объем данных в папке резервного хранилища; учитывается размер файлов в зашифрованном виде
Всего объектов	Количество объектов в резервном хранилище в текущий момент

Блокировка доступа к сетевым ресурсам. Заблокированные узлы

В этом разделе описано, как заблокировать удаленные устройства и настроить параметры хранилища заблокированных узлов.

О хранилище заблокированных узлов

Хранилище заблокированных узлов устанавливается по умолчанию, если установлен любой из следующих компонентов: Постоянная защита файлов или Защита от сетевых угроз. Эти компоненты обнаруживают попытки удаленных узлов зашифровать, открыть или исполнить файлы в папках общего доступа защищаемого устройства или сетевого хранилища в соответствии со списком заблокированных узлов. Информация о заблокированных узлах со всех защищаемых устройств отправляется в Kaspersky Security Center. Kaspersky Embedded Systems Security блокирует доступ к папкам общего доступа на защищаемом устройстве или к папкам сетевого хранилища для всех удаленных узлов из списка заблокированных узлов.

Хранилище заблокированных узлов заполняется, когда минимум одна из следующих задач запускается в активном режиме, и выполнены указанные условия:

- Для задачи Постоянная защита файлов: обнаружена вредоносная активность со стороны устройства, обращающегося к сетевым файловым ресурсам, и в параметрах задачи Постоянная защита файлов установлен флажок **Блокировать компьютеры, с которых ведется вредоносная деятельность**.

- Для задачи Защита от сетевых угроз: обнаружена активность, характерная для сетевых атак.

После обнаружения вредоносной активности или попытки шифрования задача отправляет информацию об атакующем узле в хранилище заблокированных узлов, и программа создает событие *Предупреждение* для блокировки узла. Все попытки данного узла получить доступ к защищенным сетевым папкам общего доступа будут заблокированы.

Если локально уникальный идентификатор (LUID) атакующего узла добавлен в список заблокированных узлов, Kaspersky Embedded Systems Security определяет IP-адрес этого узла и добавляет его в список заблокированных узлов вместо локально уникального идентификатора атакующего узла.

По умолчанию Kaspersky Embedded Systems Security удаляет заблокированные узлы из списка через 30 минут после добавления в список. Доступ к сетевым файловым ресурсам для компьютеров восстанавливается автоматически после их удаления из списка заблокированных узлов. Вы можете указать период, после которого заблокированные узлы автоматически разблокируются.

В случае запрета доступа к управлению хранилищами какому-либо пользователю, хранилище заблокированных узлов останется доступным. Параметры хранилища заблокированных узлов не могут быть изменены, если у пользователя отсутствует разрешение типа **Изменение прав** для управления Kaspersky Embedded Systems Security.

Управление заблокированными узлами с помощью Плагина управления

В этом разделе описана настройка параметров заблокированных узлов с помощью интерфейса Плагина управления.

Включение блокировки недоверенных узлов

Чтобы добавить узлы, проявляющие вредоносную активность или попытки шифрования, в хранилище **Заблокированные узлы** и заблокировать этим узлам доступ к сетевым файловым ресурсам, хотя бы одна из следующих задач должна работать в активном режиме:

- Постоянная защита файлов
- Защита от сетевых угроз

Чтобы настроить задачу Постоянная защита файлов, выполните следующие действия:

1. В дереве Консоли администрирования Kaspersky Security Center разверните узел **Управляемые устройства**.
2. Выберите закладку **Политики** и откройте **<Имя политики>** > **Постоянная защита компьютера** > **Настройка** в блоке **Постоянная защита файлов**.

   Откроется окно **Постоянная защита компьютера**.
3. В разделе **Интеграция с другими компонентами** установите флажок **Вносить компьютеры, с которых ведется вредоносная активность, в список недоверенных**, если требуется, чтобы программа Kaspersky Embedded Systems Security блокировала доступ к сетевым файловым ресурсам для компьютеров, со стороны которых в ходе работы задачи Постоянная защита файлов обнаружена вредоносная активность.
4. Если задача не была запущена, выберите закладку **Управление задачей**:
   a. Установите флажок **Запускать задачу по расписанию**.
   b. В раскрывающемся списке выберите частоту запуска **При запуске программы**.
5. В окне **Постоянная защита компьютера** нажмите на кнопку **ОК**.

Настроенные параметры задачи будут сохранены.

Настройте задачу Защита от сетевых угроз:

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой вы хотите настроить задачу.
3. Выберите закладку **Политики**.
4. Откройте окно свойств политики двойным щелчком мыши на имени политики, которую вы хотите настроить.
5. В открывшемся окне **Свойства: <Имя политики>** перейдите в раздел.
6. Нажмите на кнопку **Настройка** в подразделе **Защита от сетевых угроз**.

   Откроется окно **Защита от сетевых угроз**.
7. Выберите закладку **Общие**.
8. В разделе **Режим работы** выберите режим **Блокировать соединения при обнаружении атаки**.

   Флажок включает или выключает добавление узлов, проявляющих активность, характерную для сетевых атак, в список заблокированных узлов.

   Если выбран этот режим, Kaspersky Embedded Systems Security проверяет входящий сетевой трафик на наличие активности, характерной для сетевых атак, фиксирует в журнале события об обнаруженной активности и добавляет IP-адреса узлов, проявляющих активность, характерную для сетевых атак, в список заблокированных узлов.

   Этот режим выбран по умолчанию.

   Список заблокированных узлов можно просмотреть в хранилище заблокированных узлов.

   Можно восстановить доступ к заблокированным узлам, а также указать количество суток, часов и минут, по истечении которых с момента блокировки узлы получают доступ к сетевым файловым ресурсам, настроив параметры хранилища заблокированных узлов.
9. Если задача не была запущена, выберите закладку **Управление задачей**:
   a. Установите флажок **Запускать задачу по расписанию**.
   b. В раскрывающемся списке выберите частоту запуска **При запуске программы**.
10. В окне нажмите на кнопку **ОК**.
11. Настроенные параметры задачи будут сохранены.

Настройка параметров хранилища заблокированных узлов

Чтобы настроить хранилище заблокированных узлов, выполните следующие действия:

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить параметры программы.
3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
   - Чтобы настроить параметры программы для группы защищаемых устройств, выберите закладку **Политики** и откройте окно **Свойства: <Имя политики>**.
   - Чтобы настроить параметры программы для отдельного защищаемого устройства, выберите закладку **Устройства** и откройте окно **Параметры программы**.

     Если к устройству применяется активная политика Kaspersky Security Center, запрещающая изменение параметров программы, эти параметры недоступны для изменения в окне **Параметры программы**.
4. В разделе **Дополнительные возможности** нажмите на кнопку **Настройка** в подразделе **Хранилища**.

   Откроется окно **Параметры хранилищ**.
5. В разделе **Действия** на закладке **Заблокированные узлы** укажите количество суток, часов и минут, по истечении которых с момента блокировки заблокированные узлы получают доступ к сетевым файловым ресурсам.
6. Нажмите на кнопку **ОК**.

Управление заблокированными узлами с помощью Консоли программы

В этом разделе описана настройка параметров заблокированных узлов с помощью интерфейса Консоли программы.

Включение блокировки недоверенных узлов

Чтобы добавить узлы, проявляющие вредоносную активность или попытки шифрования, в хранилище **Заблокированные узлы** и заблокировать этим узлам доступ к сетевым файловым ресурсам, хотя бы одна из следующих задач должна работать в активном режиме:

- Постоянная защита файлов
- Защита от сетевых угроз

Чтобы настроить задачу Постоянная защита файлов, выполните следующие действия:

1. В дереве Консоли программы разверните узел **Постоянная защита компьютера**.
2. Выберите вложенный узел **Постоянная защита файлов**.
3. В панели результатов перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи**.

4. В разделе **Интеграция с другими компонентами** установите флажок **Блокировать компьютеры, с которых ведется вредоносная деятельность**, если вы хотите, чтобы программа Kaspersky Embedded Systems Security блокировала узлы, проявляющие вредоносную активность, во время выполнения задачи Постоянная защита файлов.

5. Если задача не была запущена, выберите закладку **Расписание**:

   a. Установите флажок **Запускать задачу по расписанию**.

   b. В раскрывающемся списке выберите частоту запуска **При запуске программы**.

6. В окне **Параметры задачи** нажмите на кнопку **ОК**.

Настроенные параметры задачи будут сохранены.

Настройте задачу Защита от сетевых угроз:

1. В дереве Консоли программы разверните узел **Постоянная защита компьютера**.

2. Выберите вложенный узел **Защита от сетевых угроз**.

3. В панели результатов узла **Защита от сетевых угроз** перейдите по ссылке **Свойства**.

4. Откроется окно **Параметры задачи**.

5. Выберите закладку **Общие**.

6. В разделе **Режим работы** выберите режим **Блокировать соединения при обнаружении атаки**.

   Флажок включает или выключает добавление узлов, проявляющих активность, характерную для сетевых атак, в список заблокированных узлов.

   Если выбран этот режим, Kaspersky Embedded Systems Security проверяет входящий сетевой трафик на наличие активности, характерной для сетевых атак, фиксирует в журнале события об обнаруженной активности и добавляет IP-адреса узлов, проявляющих активность, характерную для сетевых атак, в список заблокированных узлов.

   Этот режим выбран по умолчанию.

   Список заблокированных узлов можно просмотреть в хранилище заблокированных узлов.

   Можно восстановить доступ к заблокированным узлам, а также указать количество суток, часов и минут, по истечении которых с момента блокировки узлы получают доступ к сетевым файловым ресурсам, настроив параметры хранилища заблокированных узлов.

7. Установите или снимите флажок **Не останавливать анализ трафика, если задача не исполняется**.

   Если флажок установлен, то даже при остановке выполнения задачи Защита от сетевых угроз, Kaspersky Embedded Systems Security проверяет входящий сетевой трафик на действия, характерные для сетевых атак, и блокирует сетевую активность со стороны атакующего компьютера в выбранном режиме обработки.

   Если флажок снят, то при остановке задачи Защита от сетевых угроз, Kaspersky Embedded Systems Security не проверяет входящий сетевой трафик на действия, характерные для сетевых атак, и не блокирует сетевую активность со стороны атакующего компьютера.

   По умолчанию флажок снят.

8. Если задача не была запущена, выберите закладку **Расписание**:

   a. Установите флажок **Запускать задачу по расписанию**.

   b. В раскрывающемся списке выберите частоту запуска **При запуске программы**.

9. В окне **Параметры задачи** нажмите на кнопку **OK**.

Настроенные параметры задачи будут сохранены.

Настройка параметров хранилища заблокированных узлов

Чтобы настроить хранилище заблокированных узлов, выполните следующие действия:

1. В дереве Консоли программы разверните узел **Хранилища**.
2. Откройте контекстное меню вложенного узла **Заблокированные узлы**.
3. Выберите пункт меню **Свойства**.

   Откроется окно **Параметры хранилища заблокированных узлов**.
4. В разделе **Действия** укажите количество суток, часов и минут, по истечении которых с момента блокировки заблокированные узлы получают доступ к сетевым файловым ресурсам.
5. Нажмите на кнопку **OK**.
6. Чтобы восстановить доступ для всех заблокированных узлов, выполните следующие действия:

   a. Откройте контекстное меню вложенного узла **Заблокированные узлы**.

   b. Выберите пункт **Разблокировать все**.

   Все узлы будут удалены из списка и разблокированы.
7. Чтобы удалить узлы из списка заблокированных, выполните следующие действия:

   a. В списке заблокированных узлов в панели результатов выберите один или несколько узлов.

   b. Откройте контекстное меню вложенного узла **Заблокированные узлы**.

   c. Выберите пункт **Разблокировать выбранное**.

   Выбранные узлы будут разблокированы.

Управление заблокированными узлами с помощью Веб-плагина

В этом разделе описана настройка параметров заблокированных узлов с помощью интерфейса Веб-плагина.

Включение блокировки узлов

Чтобы добавить узлы, проявляющие вредоносную активность или попытки шифрования, в хранилище **Заблокированные узлы** и заблокировать этим узлам доступ к сетевым файловым ресурсам, хотя бы одна из следующих задач должна работать в активном режиме:

- Постоянная защита файлов
- Защита от сетевых угроз

Чтобы настроить задачу Постоянная защита файлов, выполните следующие действия:

1. В главном окне веб-консоли выберите **Устройства** → **Политики и профили**.
2. Выберите политику, которую вы хотите настроить.
3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.
4. Перейдите в раздел **Постоянная защита компьютера**.
5. Нажмите на кнопку **Параметры** в подразделе **Постоянная защита файлов**.
6. В разделе **Интеграция с другими компонентами** установите флажок **Блокировать доступ к сетевым файловым ресурсам для узлов, с которых ведется вредоносная активность**, если вы хотите, чтобы программа Kaspersky Embedded Systems Security блокировала доступ к сетевым файловым ресурсам для узлов, проявляющих вредоносную активность, во время выполнения задачи Постоянная защита файлов.
7. Если задача не была запущена, выберите закладку **Управление задачей**:
   a. Установите флажок **Запускать задачу по расписанию**.
   b. В раскрывающемся списке выберите частоту запуска **При запуске программы**.
8. Нажмите на кнопку **Сохранить**.

Настроенные параметры задачи будут сохранены.

Настройка параметров хранилища заблокированных узлов

Чтобы настроить хранилище заблокированных узлов, выполните следующие действия:

1. В главном окне веб-консоли выберите **Устройства** → **Политики и профили**.
2. Выберите политику, которую вы хотите настроить.
3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.
4. Выберите раздел **Дополнительные возможности**.
5. Нажмите на кнопку **Параметры** в подразделе **Хранилища**.
6. В разделе **Дополнительные возможности** нажмите на кнопку **Настройка** в подразделе **Хранилища**.

   Откроется окно **Хранилища**.
7. В разделе **Действия** на закладке **Заблокированные узлы** укажите количество суток, часов и минут, по истечении которых с момента блокировки заблокированные узлы получают доступ к сетевым файловым

ресурсам.

8. Нажмите на кнопку **OK**.

Запись событий. Журналы Kaspersky Embedded Systems Security

Этот раздел содержит информацию о работе с журналами Kaspersky Embedded Systems Security: журналом системного аудита, журналами выполнения задач и журналом событий.

Способы записи событий Kaspersky Embedded Systems Security

События Kaspersky Embedded Systems Security делятся на две группы:

- события, связанные с обработкой объектов в задачах Kaspersky Embedded Systems Security;
- события, связанные с управлением Kaspersky Embedded Systems Security, например: запуск программы, создание или удаление задач, изменение параметров задач.

Kaspersky Embedded Systems Security использует следующие способы записи событий:

- **Журналы выполнения задач**. Журнал выполнения задачи содержит информацию о текущем состоянии задачи и событиях, возникших за время ее выполнения.
- **Журнал системного аудита**. Журнал системного аудита содержит информацию о событиях, связанных с управлением Kaspersky Embedded Systems Security.
- **Журнал событий**. Журнал событий содержит информацию о событиях, которые нужны для диагностики сбоев в работе Kaspersky Embedded Systems Security. Журнал событий доступен в "Просмотре событий" Microsoft Windows.
- **Журнал событий безопасности**. Журнал безопасности содержит информацию о событиях, связанных с нарушениями безопасности или с попытками нарушения безопасности на защищаемом устройстве.

Если в работе Kaspersky Embedded Systems Security возникла проблема (например, Kaspersky Embedded Systems Security или отдельная задача завершилась аварийно или не запустилась), то для ее диагностики можно создать файл трассировки и файл дампа процессов Kaspersky Embedded Systems Security и отправить файлы с этой информацией на анализ в Службу технической поддержки "Лаборатории Касперского".

Kaspersky Embedded Systems Security не отправляет файлы трассировки и файлы дампов автоматически. Диагностические данные могут быть отправлены только пользователем с соответствующими правами.

Kaspersky Embedded Systems Security записывает информацию в файлы трассировки и файлы дампов в незашифрованном виде. Папка, в которую сохраняются файлы, выбирается пользователем и контролируется параметрами операционной системы и Kaspersky Embedded Systems Security. Можно настроить права доступа и разрешить доступ к журналам, файлам трассировки и файлам дампов только для выбранных пользователей.

Журнал системного аудита

Kaspersky Embedded Systems Security ведет системный аудит событий, связанных с управлением Kaspersky Embedded Systems Security. Программа сохраняет информацию, например, о запуске программы, запуске и остановке задач Kaspersky Embedded Systems Security, изменении параметров задач, создании и удалении задач проверки по требованию. Записи об этих событиях отображаются в панели результатов при выборе узла **Журнал системного аудита** в Консоли программы.

По умолчанию Kaspersky Embedded Systems Security хранит записи в журнале системного аудита без ограничения срока хранения. Вы можете установить срок хранения записей в журнале системного аудита.

Вы можете указать папку, в которую Kaspersky Embedded Systems Security будет сохранять файлы журнала системного аудита, отличную от папки, установленной по умолчанию.

Сортировка событий в журнале системного аудита

По умолчанию события отображаются в журнале системного аудита в обратном хронологическом порядке.

Вы можете отсортировать события по содержимому любой графы, кроме графы **Событие**.

Чтобы отсортировать события в журнале системного аудита, выполните следующие действия:

1. В дереве Консоли программы разверните узел **Журналы и уведомления**.
2. Выберите вложенный узел **Журнал системного аудита**.
3. В панели результатов выберите заголовок графы, по содержимому которой вы хотите отсортировать события в таблице.

Результат сортировки сохранится до следующего просмотра журнала системного аудита.

Фильтрация событий в журнале системного аудита

Вы можете отобразить в журнале системного аудита записи только о тех событиях, которые удовлетворяют заданным условиям фильтрации (фильтрам).

Чтобы отфильтровать события в журнале системного аудита, выполните следующие действия:

1. В дереве Консоли программы разверните узел **Журналы и уведомления**.
2. Откройте контекстное меню вложенного узла **Журнал системного аудита** и выберите пункт **Фильтр**.

   Откроется окно **Параметры фильтра**.
3. Чтобы добавить фильтр, выполните следующие действия:
   a. В списке **Название поля** выберите графу, по которой вы хотите отфильтровать события.
   b. В списке **Оператор** выберите условие фильтрации. Условия фильтрации различаются в зависимости от элемента, выбранного в списке **Название поля**.
   c. В списке **Значение поля** выберите значение фильтра.
   d. Нажмите на кнопку **Добавить**.

Добавленный фильтр отобразится в списке фильтров в окне **Параметры фильтра**.

4. Если требуется, выполните одно из следующих действий:

   - Чтобы объединить несколько фильтров по логическому "И", выберите вариант **При выполнении всех условий**.
   - Чтобы объединить несколько фильтров по логическому "ИЛИ", выберите вариант **При выполнении любого условия**.

5. Нажмите на кнопку **Применить**, чтобы сохранить условия фильтрации событий в журнале системного аудита.

   В списке событий журнала системного аудита отобразятся только события, которые удовлетворяют условиям фильтрации. Результат фильтрации сохранится до следующего просмотра журнала системного аудита.

Чтобы выключить действие фильтра, выполните следующие действия:

1. В дереве Консоли программы разверните узел **Журналы и уведомления**.
2. Откройте контекстное меню вложенного узла **Журнал системного аудита** и выберите пункт **Снять фильтр**.

   В списке событий журнала системного аудита отобразятся все события.

Удаление событий из журнала системного аудита

По умолчанию Kaspersky Embedded Systems Security хранит записи в журнале системного аудита без ограничения срока хранения. Вы можете установить срок хранения записей в журнале системного аудита.

Вы можете вручную удалить все события из журнала системного аудита.

Чтобы удалить события из журнала системного аудита, выполните следующие действия:

1. В дереве Консоли программы разверните узел **Журналы и уведомления**.
2. Откройте контекстное меню вложенного узла **Журнал системного аудита** и выберите пункт **Очистить**.
3. Выполните одно из следующих действий:

   - Если вы хотите перед удалением событий из журнала системного аудита сохранить содержимое журнала в файл в формате CSV или TXT, в окне подтверждения удаления нажмите на кнопку **Да**. В открывшемся окне укажите имя и местоположение файла.
   - Если вы не хотите сохранить содержимое журнала в файл, в окне подтверждения удаления нажмите на кнопку **Нет**.

Журнал системного аудита будет очищен.

Журналы выполнения задач

Этот раздел содержит информацию о журналах выполнения задач Kaspersky Embedded Systems Security и инструкции по работе с ними.

О журналах выполнения задач

Информация о выполнении задач Kaspersky Embedded Systems Security отображается в панели результатов при выборе узла **Журналы выполнения задач** в Консоли программы.

В журнале выполнения каждой задачи можно просмотреть статистику выполнения задачи, информацию о каждом объекте, который был обработан программой с момента запуска задачи, а также параметры задачи.

По умолчанию Kaspersky Embedded Systems Security хранит записи в журналах выполнения задач в течение 30 дней с момента завершения задачи. Вы можете изменять длительность хранения записей в журналах выполнения задач.

Вы можете указать папку, в которой Kaspersky Embedded Systems Security сохраняет файлы журналов выполнения задач, отличную от папки, установленной по умолчанию. Можно также выбрать события, записи о которых Kaspersky Embedded Systems Security сохраняет в журналах выполнения задач.

Просмотр списка событий в журналах выполнения задач

Чтобы просмотреть журналы выполнения задач, выполните следующие действия:

1. В дереве Консоли программы разверните узел **Журналы и уведомления**.
2. Выберите вложенный узел **Журналы выполнения задач**.

   Список событий, сохраненных в журналах выполнения задач Kaspersky Embedded Systems Security, отобразится в панели результатов.

Вы можете отсортировать события по содержимому любой графы или применить фильтр.

Сортировка журналов выполнения задач

По умолчанию журналу выполнения задач отображаются в обратном хронологическом порядке. Вы можете отсортировать события по содержимому любой графы.

Чтобы отсортировать журналы выполнения задач, выполните следующие действия:

1. В дереве Консоли программы разверните узел **Журналы и уведомления**.
2. Выберите вложенный узел **Журналы выполнения задач**.
3. В панели результатов выберите заголовок графы, по содержимому которой вы хотите отсортировать журналы выполнения задач Kaspersky Embedded Systems Security.

   Результат сортировки сохранится до следующего просмотра журналов выполнения задач.

Фильтрация журналов выполнения задач

Вы можете настроить отображение в списке журналов выполнения задач только журналы, которые удовлетворяют заданным условиям фильтрации (фильтрам).

Чтобы отфильтровать журналы выполнения задач, выполните следующие действия:

1. В дереве Консоли программы разверните узел **Журналы и уведомления**.
2. Откройте контекстное меню вложенного узла **Журналы выполнения задач** и выберите пункт **Фильтр**.

   Откроется окно **Параметры фильтра**.
3. Чтобы добавить фильтр, выполните следующие действия:

   a. В списке **Название поля** выберите графу, по которой вы хотите отфильтровать журналы выполнения задач.

   b. В списке **Оператор** выберите условие фильтрации. Условия фильтрации различаются в зависимости от элемента, выбранного в списке **Название поля**.

   c. В списке **Значение поля** выберите значение фильтра.

   d. Нажмите на кнопку **Добавить**.

   Добавленный фильтр отобразится в списке фильтров в окне **Параметры фильтра**.
4. Если требуется, выполните одно из следующих действий:

   - Чтобы объединить несколько фильтров по логическому "И", выберите вариант **При выполнении всех условий**.
   - Чтобы объединить несколько фильтров по логическому "ИЛИ", выберите вариант **При выполнении любого условия**.
5. Нажмите на кнопку **Применить**, чтобы сохранить условия фильтрации в списке журналов выполнения задач.

В списке журналов выполнения задач отобразятся только журналы, которые удовлетворяют условиям фильтрации. Результат фильтрации сохранится до следующего просмотра журналов выполнения задач.

Чтобы выключить действие фильтра, выполните следующие действия:

1. В дереве Консоли программы разверните узел **Журналы и уведомления**.
2. Откройте контекстное меню вложенного узла **Журналы выполнения задач** и выберите пункт **Снять фильтр**.

В списке журналов выполнения задач отобразятся все журналы.

Просмотр статистики и информации о задачах Kaspersky Embedded Systems Security в журналах выполнения задач

В журналах выполнения задач вы можете просмотреть подробную информацию обо всех событиях, возникших в задачах с момента их запуска, а также статистику выполнения задач и параметры задач.

Чтобы просмотреть статистику и информацию о задаче Kaspersky Embedded Systems Security , выполните следующие действия:

1. В дереве Консоли программы разверните узел **Журналы и уведомления**.

2. Выберите вложенный узел **Журналы выполнения задач**.

3. В панели результатов откройте окно **Журнал выполнения** одним из следующих способов:

   - двойным щелчком мыши на его имени журнала выполнения задачи, который вы хотите просмотреть;
   - выбрав пункт **Просмотреть журнал** в контекстном меню журнала, который вы хотите просмотреть.

4. В открывшемся окне отображается следующая информация:

   - На закладке **Статистика** отображается время запуска и завершения задачи и ее статистика.
   - На закладке **События** отображается список событий, зафиксированных во время выполнения задачи.
   - На закладке **Параметры** отображаются параметры задачи.

5. Если требуется, нажмите на кнопку **Фильтр**, чтобы отфильтровать события в журнале выполнения задачи.

6. Если требуется, нажмите на кнопку **Экспорт**, чтобы экспортировать информацию из журнала выполнения задачи в файл в CSV- или TXT-формате.

7. Нажмите на кнопку **Закрыть**.

   Окно **Журнал выполнения** будет закрыто.

Экспорт информации из журнала выполнения задачи

Вы можете экспортировать информацию из журнала выполнения задачи в файл в CSV- или TXT-формате.

Чтобы экспортировать информацию из журнала выполнения задачи, выполните следующие действия:

1. В дереве Консоли программы разверните узел **Журналы и уведомления**.

2. Выберите вложенный узел **Журналы выполнения задач**.

3. В панели результатов откройте окно **Журнал выполнения** одним из следующих способов:

   - двойным щелчком мыши на его имени журнала выполнения задачи, который вы хотите просмотреть;
   - выбрав пункт **Просмотреть журнал** в контекстном меню журнала, который вы хотите просмотреть.

4. В нижней части окна **Журнал выполнения** нажмите на кнопку **Экспорт**.

   Откроется окно **Сохранить как**.

5. Укажите имя, местоположение, тип и кодировку файла, в который вы хотите экспортировать информацию из журнала выполнения задачи.

6. Нажмите на кнопку **Сохранить**.

   Настроенные параметры будут сохранены.

Удаление журналов выполнения задач

По умолчанию Kaspersky Embedded Systems Security хранит записи в журналах выполнения задач в течение 30 дней с момента завершения задачи. Вы можете изменять длительность хранения записей в журналах выполнения задач.

Можно вручную удалить журналы выполнения завершившихся задач.

> События из журналов задач, выполняющихся в данный момент, и задач, используемых другими пользователями, удалены не будут.

Чтобы удалить журналы выполнения задач, выполните следующие действия:

1. В дереве Консоли программы разверните узел **Журналы и уведомления**.
2. Выберите вложенный узел **Журналы выполнения задач**.
3. Выполните одно из следующих действий:
   - Чтобы удалить журналы выполнения всех завершившихся задач, откройте контекстное меню вложенного узла **Журналы выполнения задач** и выберите пункт **Очистить**.
   - Чтобы очистить журнал выполнения отдельной задачи, в панели результатов откройте контекстное меню журнала, который вы хотите очистить, и выберите пункт **Удалить**.
   - Чтобы очистить журналы выполнения нескольких задач, выполните следующие действия:
     a. В панели результатов с помощью клавиш **CTRL** и **SHIFT** выберите журналы выполнения задач, которые вы хотите очистить.
     b. Откройте контекстное меню любого журнала выполнения задач и выберите пункт **Удалить**.
4. В окне подтверждения удаления нажмите на кнопку **Да**, чтобы подтвердить удаление журналов.

Выбранные журналы выполнения задач будут очищены. Удаление журналов выполнения задач будет зарегистрировано в журнале системного аудита.

Журнал безопасности

Kaspersky Embedded Systems Security ведет журнал событий, связанных с нарушениями безопасности или попытками нарушения безопасности на защищаемом устройстве. В данном журнале фиксируются следующие события:

- События компонента Защита от эксплойтов.
- Критические события компонента Анализ журналов.
- Критические события, свидетельствующие о попытке нарушения безопасности (для задач Постоянная защита компьютера, Проверка по требованию, Мониторинг файловых операций, Контроль запуска программ и Контроль устройств).

Вы можете очистить журнал безопасности и журнал системного аудита. При очистке журнала безопасности Kaspersky Embedded Systems Security регистрирует событие системного аудита.

Просмотр журнала событий Kaspersky Embedded Systems Security в оснастке Просмотр событий

С помощью оснастки Просмотр событий в Microsoft Management Console можно просматривать журнал событий Kaspersky Embedded Systems Security. В журнале содержатся события, зарегистрированные Kaspersky Embedded Systems Security и необходимые для диагностики сбоев в работе программы.

Вы можете выбирать события для записи в журнал событий на основе следующих критериев:

- **по типам событий**;
- **по уровню детализации**. Уровень детализации соответствует уровню важности событий, которые регистрируются в журнале (информационные, важные или критические события). Наиболее подробным является уровень Информационные события, при котором регистрируются все события. Наименее подробным является уровень Критические события, при котором регистрируются только критические события.

Чтобы просмотреть журнал событий Kaspersky Embedded Systems Security, выполните следующие действия:

1. Нажмите на кнопку **Пуск**, введите в поисковой строке команду `mmc` и нажмите на клавишу **ENTER**.

   Откроется Microsoft Management Console.

2. Выберите **Файл** > **Добавить или удалить оснастку**.

   Откроется окно **Добавление и удаление оснасток**.

3. В списке доступных оснасток выберите оснастку **Просмотр событий** и нажмите на кнопку **Добавить**.

   Откроется окно **Выбор компьютера**.

4. В окне **Выбор компьютера** укажите защищаемое устройство, на котором установлена программа Kaspersky Embedded Systems Security, и нажмите на кнопку **OK**.

5. В окне **Добавление и удаление оснасток** нажмите на кнопку **OK**.

   В дереве Microsoft Management Console появится узел **Просмотр событий**.

6. Раскройте узел **Просмотр событий** и выберите вложенный узел **Журналы приложений и служб** > **Kaspersky Embedded Systems Security.**

Откроется журнал событий Kaspersky Embedded Systems Security.

Настройка параметров журналов с помощью Плагина управления

Вы можете настраивать следующие параметры журналов Kaspersky Embedded Systems Security:

- длительность хранения событий в журналах выполнения задач и журнале системного аудита;
- местоположение папки, в которой Kaspersky Embedded Systems Security сохраняет файлы журналов выполнения задач и журнала системного аудита;
- пороги формирования событий *Базы программы устарели*, *Базы программы сильно устарели* и *Проверка важных областей защищаемого устройства давно не выполнялась*;

- события, которые Kaspersky Embedded Systems Security сохраняет в журналах выполнения задач, журнале системного аудита и журнале событий Kaspersky Embedded Systems Security в оснастке Просмотр событий;

- параметры публикации событий аудита и событий выполнения задач по протоколу syslog на syslog-сервер.

Чтобы настроить параметры журналов Kaspersky Embedded Systems Security, выполните следующие действия:

1. В дереве Консоли программы откройте контекстное меню узла **Журналы и уведомления** и выберите пункт **Свойства**.

   Откроется окно **Параметры журналов и уведомлений**.

2. В окне **Параметры журналов и уведомлений** настройте параметры журналов в соответствии с вашими требованиями. Для этого выполните следующие действия:

   - На закладке **Общие**, если требуется, выберите события, которые Kaspersky Embedded Systems Security сохраняет в журналах выполнения задач, журнале системного аудита и журнале событий Kaspersky Embedded Systems Security в оснастке Просмотр событий. Для этого выполните следующие действия:

     - В списке **Компонент** выберите компонент Kaspersky Embedded Systems Security, уровень детализации событий которого вы хотите указать.

     > Для компонентов Постоянная защита файлов, Проверка по требованию и Обновление предусмотрена запись событий в журналы выполнения задач и журнал событий. Для этих компонентов таблица событий содержит графы **Журнал выполнения задачи** и **Журнал событий Windows**. Для компонентов Карантин и Резервное хранилище события записываются в журнал системного аудита и журнал событий. Для этих компонентов таблица событий содержит графы **Системный аудит** и **Журнал событий Windows**.

     - В списке **Уровень важности** выберите уровень детализации событий в журналах выполнения задач, журнале системного аудита и журнале событий для выбранного компонента.

       В таблице событий флажки установлены рядом с событиями, которые регистрируются в журналах выполнения задач, журнале системного аудита и журнале событий в соответствии с выбранным уровнем детализации.

     - Если вы хотите вручную включить запись отдельных событий для выбранного функционального компонента, выполните следующие действия:

     a. В списке **Уровень важности** выберите **Другой**.

     b. В таблице списка событий установите флажки рядом с теми событиями, запись которых в журналы выполнения задач, журнал системного аудита и журнал событий вы хотите включить.

   - На закладке **Дополнительно** настройте параметры хранения журналов и пороги формирования событий для состояния защиты устройства:

     - В разделе **Хранение журналов**:

       - **Папка с журналами**

       - **Удалять события в журналах выполнения задач старше, чем (сут)**

- **Удалять события в журнале системного аудита старше, чем (сут)**

- В разделе **Пороги формирования событий**:

  - Укажите количество дней, по истечении которого будут регистрироваться события *Базы программы устарели*, *Базы программы сильно устарели* и *Проверка важных областей защищаемого устройства давно не выполнялась*.

- На закладке **Интеграция с SIEM** настройте параметры публикации событий аудита и событий выполнения задач на syslog-сервере.

3. Нажмите на кнопку **OK**, чтобы сохранить изменения.

Об интеграции с SIEM

Чтобы уменьшить нагрузку на маломощные устройства и уменьшить риск снижения производительности системы в результате увеличения размеров журналов программы, можно настроить публикацию событий аудита и событий выполнения задач по протоколу syslog на *syslog-сервер*.

Syslog-сервер – это внешний сервер для сбора событий (SIEM). Он собирает и анализирует полученные события, а также выполняет другие действия по управлению журналами.

Вы можете использовать интеграцию с SIEM в двух режимах:

- Дублировать события на syslog-сервере: в этом режиме все события выполнения задач, публикация которых настроена в параметрах журналов, а также все события системного аудита продолжают храниться на защищаемом устройстве даже после отправки на SIEM-сервер.

  Рекомендуется использовать этот режим, чтобы максимально снизить нагрузку на защищаемое устройство.

- Удалять локальные копии событий: в этом режиме все события, зарегистрированные в ходе работы программы и опубликованные на SIEM-сервере, будут удалены с защищаемого устройства.

  > Программа никогда не удаляет локальные версии журнала безопасности.

Kaspersky Embedded Systems Security может конвертировать события в журналах программы в форматы, поддерживаемые syslog-сервером, для передачи событий и их успешного распознавания на стороне SIEM-сервера. Программа поддерживает конвертацию в формат структурированных данных и в формат JSON.

Рекомендуется выбирать формат событий на основе конфигурации используемого SIEM-сервера.

Параметры надежности

Чтобы снизить риск неудачной отправки событий на SIEM-сервер, задайте параметры подключения к зеркальному syslog-серверу.

Зеркальный syslog-сервер – это дополнительный syslog-сервер, на использование которого программа переключается автоматически, если не удается подключиться к основному syslog-серверу или использовать его.

Также Kaspersky Embedded Systems Security использует события системного аудита для уведомления о неудачных попытках подключения к SIEM-серверу и об ошибках отправки событий на SIEM-сервер.

Настройка параметров интеграции с SIEM

Интеграция с SIEM не применяется по умолчанию. Вы можете включать и выключать интеграцию с SIEM, а также настраивать соответствующие параметры (см. таблицу ниже).

Параметры интеграции с SIEM

Параметр	Значение по умолчанию	Описание
Отправлять события по протоколу syslog на внешний syslog-сервер	Не применяется	Вы можете включать и отключать интеграцию с SIEM с помощью установки или снятия флажка.
Удалять локальные копии событий при записи на внешний syslog-сервер	Не применяется	Вы можете настраивать параметры хранения локальных копий журналов после их отправки на SIEM-сервер, установив или сняв флажок.
Формат событий	Структурированные данные	Вы можете выбирать один из двух форматов, в которые программа конвертирует события перед отправкой на syslog-сервер для лучшего распознавания этих событий SIEM-сервером.
Протокол подключения	TCP	Вы можете настроить подключение к основному и дополнительному syslog-серверам по протоколам UPD или TCP с помощью выпадающего списка.
Параметры подключения к основному syslog-серверу	IP-адрес: 127.0.0.1 Порт: 514	Вы можете настраивать значения IP-адреса и порта для подключения к основному syslog-серверу с помощью соответствующих полей. Вы можете указать значение IP-адреса только в формате IPv4.
Использовать дополнительный syslog-сервер, если основной syslog-сервер недоступен	Не применяется	Вы можете включать и отключать применение зеркального syslog-сервера с помощью флажка.
Параметры подключения к дополнительному syslog-серверу	IP-адрес: 127.0.0.1 Порт: 514	Вы можете настраивать значения IP-адреса и порта для подключения к дополнительному syslog-серверу с помощью соответствующих полей. Вы можете указать значение IP-адреса только в формате IPv4.

Чтобы настроить параметры интеграции с SIEM, выполните следующие действия:

1. В дереве Консоли программы откройте контекстное меню узла **Журналы и уведомления**.
2. Выберите пункт **Свойства**.

   Откроется окно **Параметры журналов и уведомлений**.
3. Выберите закладку **Интеграция с SIEM**.
4. В разделе **Параметры интеграции** установите флажок **Отправлять события по протоколу syslog на внешний syslog-сервер**.

5. Если требуется, в разделе **Параметры интеграции** установите флажок **Удалять локальные копии событий при записи на внешний syslog-сервер**.

   Статус флажка **Удалять локальные копии событий при записи на внешний syslog-сервер** не влияет на параметры хранения событий журнала безопасности: программа никогда не удаляет события журнала безопасности автоматически.

6. В разделе **Формат событий** укажите формат, в который вы хотите конвертировать события программы для их отправки на SIEM-сервер.

   По умолчанию программа выполняет конвертацию в формат структурированных данных.

7. В разделе **Параметры принимающего syslog-сервера**:

   - Укажите протокол подключения к SIEM.
   - Укажите параметры соединения с основным syslog-сервером.

     IP-адрес можно указать только в формате IPv4.
   - Установите флажок **Использовать дополнительный syslog-сервер, если основной syslog-сервер недоступен**, если вы хотите, чтобы программа использовала другие параметры соединения, когда отправка событий на основной syslog-сервер невозможна.

     Укажите следующие параметры подключения к дополнительному syslog-серверу: **Адрес** и **Порт**.

     Поля **Адрес** и **Порт** для дополнительного syslog-сервера недоступны для редактирования, если снят флажок **Использовать дополнительный syslog-сервер, если основной syslog-сервер недоступен**.

     IP-адрес можно указать только в формате IPv4.

8. Нажмите на кнопку **OK**.

   Настроенные параметры интеграции с SIEM будут применены.

Настройка журналов и уведомлений

В Консоли администрирования Kaspersky Security Center можно настроить уведомление администратора и пользователей о следующих событиях, связанных с работой Kaspersky Embedded Systems Security и состоянием антивирусной защиты устройства:

- Администратор может получать информацию о событиях выбранных типов.
- Пользователи локальной сети, которые обращаются к защищаемому устройству, и пользователи терминального защищаемого устройства могут получать информацию о событиях *Обнаружен объект*.

Можно настроить уведомления о событиях Kaspersky Embedded Systems Security как для отдельного защищаемого устройства в окне **Свойства: <Имя защищаемого устройства>** выбранного защищаемого устройства, так и для группы защищаемых устройств в окне **Свойства: <Имя политики>** выбранной группы администрирования.

На закладке **Уведомления о событиях** или в окне **Настройка уведомлений** можно настроить следующие типы уведомлений:

- На закладке **Уведомления о событиях** (стандартная закладка в Kaspersky Security Center) можно настроить уведомления администратора о событиях выбранных типов. Подробная информация о способах уведомлений приведена в *Справке Kaspersky Security Center*.

- В окне **Настройка уведомлений** можно настроить уведомления как администратора, так и пользователей.

Уведомления о событиях некоторых типов можно настраивать только на закладке или только в окне, о событиях других типов – как на закладке, так и в окне.

Если вы настроите уведомления о событиях одного типа в одинаковом режиме на закладке **Уведомления о событиях** и в окне **Настройка уведомлений**, системный администратор будет получать уведомления об этих событиях дважды.

Настройка параметров журналов

Чтобы настроить параметры журналов Kaspersky Embedded Systems Security, выполните следующие действия:

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить параметры программы.
3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
   - Чтобы настроить параметры программы для группы защищаемых устройств, выберите закладку **Политики** и откройте окно **Свойства: <Имя политики>**.
   - Чтобы настроить параметры программы для отдельного защищаемого устройства, выберите закладку **Устройства** и откройте окно **Параметры программы**.

     Если к устройству применяется активная политика Kaspersky Security Center, запрещающая изменение параметров программы, эти параметры недоступны для изменения в окне **Параметры программы**.
4. В разделе **Журналы и уведомления** в подразделе **Журналы выполнения задач** нажмите на кнопку **Настройка**.
5. В окне **Параметры журналов** настройте следующие параметры Kaspersky Embedded Systems Security согласно вашим требованиям:
   - Настройте уровень детализации событий в журналах. Для этого выполните следующие действия:
     a. В списке **Компонент** выберите компонент Kaspersky Embedded Systems Security, уровень детализации событий которого вы хотите указать.
     b. Чтобы задать уровень детализации в журналах выполнения задач и в журнале системного аудита для выбранного компонента, выберите требуемый уровень в списке **Уровень важности**.
   - Чтобы изменить расположение журналов по умолчанию, укажите полный путь к папке или выберите папку с помощью кнопки **Обзор**.
   - Укажите, сколько дней будут храниться журналы выполнения задач.

- Укажите, сколько дней будет храниться информация, которая отображается в узле **Журнал системного аудита**.

6. Нажмите на кнопку **OK**.

Настроенные параметры журналов будут сохранены.

Журнал безопасности

Kaspersky Embedded Systems Security ведет журнал событий, связанных с нарушениями безопасности или попытками нарушения безопасности на защищаемом устройстве. В данном журнале фиксируются следующие события:

- События компонента Защита от эксплойтов.
- Критические события компонента Анализ журналов.
- Критические события, свидетельствующие о попытке нарушения безопасности (для задач Постоянная защита компьютера, Проверка по требованию, Мониторинг файловых операций, Контроль запуска программ и Контроль устройств).

Вы можете очистить журнал безопасности и журнал системного аудита. При очистке журнала безопасности Kaspersky Embedded Systems Security регистрирует событие системного аудита.

Настройка параметров интеграции с SIEM

Чтобы уменьшить нагрузку на маломощные устройства и уменьшить риск снижения производительности системы в результате увеличения размеров журналов программы, можно настроить публикацию событий аудита и событий выполнения задач по протоколу syslog на *syslog-сервер*.

Syslog-сервер – это внешний сервер для сбора событий (SIEM). Он собирает и анализирует полученные события, а также выполняет другие действия по управлению журналами.

Вы можете использовать интеграцию с SIEM в двух режимах:

- Дублировать события на syslog-сервере: в этом режиме все события выполнения задач, публикация которых настроена в параметрах журналов, а также все события системного аудита продолжают храниться на защищаемом устройстве даже после отправки на SIEM-сервер.

  Рекомендуется использовать этот режим, чтобы максимально снизить нагрузку на защищаемое устройство.

- Удалять локальные копии событий: в этом режиме все события, зарегистрированные в ходе работы программы и опубликованные на SIEM-сервере, будут удалены с защищаемого устройства.

  Программа никогда не удаляет локальные версии журнала безопасности.

Kaspersky Embedded Systems Security может конвертировать события в журналах программы в форматы, поддерживаемые syslog-сервером, для передачи событий и их успешного распознавания на стороне SIEM-сервера. Программа поддерживает конвертацию в формат структурированных данных и в формат JSON.

Чтобы снизить риск неудачной отправки событий на SIEM-сервер, задайте параметры подключения к зеркальному syslog-серверу.

Зеркальный syslog-сервер – это дополнительный syslog-сервер, на использование которого программа переключается автоматически, если не удается подключиться к основному syslog-серверу или использовать его.

Интеграция с SIEM не применяется по умолчанию. Вы можете включать и выключать интеграцию с SIEM, а также настраивать соответствующие параметры (см. таблицу ниже).

Параметры интеграции с SIEM

Параметр	Значение по умолчанию	Описание
Отправлять события по протоколу syslog на внешний syslog-сервер	Не применяется	Вы можете включать и отключать интеграцию с SIEM с помощью установки или снятия флажка.
Удалять локальные копии событий при записи на внешний syslog-сервер	Не применяется	Вы можете настраивать параметры хранения локальных копий журналов после их отправки на SIEM-сервер, установив или сняв флажок.
Формат событий	Структурированные данные	Вы можете выбирать один из двух форматов, в которые программа конвертирует события перед отправкой на syslog-сервер для лучшего распознавания этих событий SIEM-сервером.
Протокол подключения	TCP	С помощью выпадающего списка вы можете настроить подключение к основному syslog-серверу по протоколам UPD или TCP, к дополнительному syslog-серверу по протоколу TCP.
Параметры подключения к основному syslog-серверу	IP-адрес: 127.0.0.1 Порт: 514	Вы можете настраивать значения IP-адреса и порта для подключения к основному syslog-серверу с помощью соответствующих полей. Вы можете указать значение IP-адреса только в формате IPv4.
Использовать дополнительный syslog-сервер, если основной syslog-сервер недоступен	Не применяется	Вы можете включать и отключать применение зеркального syslog-сервера с помощью флажка.
Параметры подключения к дополнительному syslog-серверу	IP-адрес: 127.0.0.1 Порт: 514	Вы можете настраивать значения IP-адреса и порта для подключения к дополнительному syslog-серверу с помощью соответствующих полей. Вы можете указать значение IP-адреса только в формате IPv4.

Чтобы настроить параметры интеграции с SIEM, выполните следующие действия:

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.

2. Выберите группу администрирования, для которой требуется настроить параметры программы.

3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:

   - Чтобы настроить параметры программы для группы защищаемых устройств, выберите закладку **Политики** и откройте окно **Свойства: <Имя политики>**.

- Чтобы настроить параметры программы для отдельного защищаемого устройства, выберите закладку **Устройства** и откройте окно **Параметры программы**.

  Если к устройству применяется активная политика Kaspersky Security Center, запрещающая изменение параметров программы, эти параметры недоступны для изменения в окне **Параметры программы**.

4. В разделе **Журналы и уведомления** в подразделе **Журналы выполнения задач** нажмите на кнопку **Настройка**.

   Откроется окно **Параметры журналов и уведомлений**.

5. Выберите закладку **Интеграция с SIEM**.

6. В разделе **Параметры интеграции** установите флажок **Отправлять события по протоколу syslog на внешний syslog-сервер**.

7. Если требуется, в разделе **Параметры интеграции** установите флажок **Удалять локальные копии событий при записи на внешний syslog-сервер**.

   Статус флажка **Удалять локальные копии событий при записи на внешний syslog-сервер** не влияет на параметры хранения событий журнала безопасности: программа никогда не удаляет события журнала безопасности автоматически.

8. В разделе **Формат событий** укажите формат, в который вы хотите конвертировать события программы для их отправки на SIEM-сервер.

   По умолчанию программа выполняет конвертацию в формат структурированных данных.

9. В разделе **Параметры принимающего syslog-сервера**:

   - Укажите протокол подключения к SIEM.
   - Укажите параметры соединения с основным syslog-сервером.

     IP-адрес можно указать только в формате IPv4.
   - Установите флажок **Использовать дополнительный syslog-сервер, если основной syslog-сервер недоступен**, если вы хотите, чтобы программа использовала другие параметры соединения, когда отправка событий на основной syslog-сервер невозможна.

     Укажите следующие параметры подключения к дополнительному syslog-серверу: **Адрес** и **Порт**.

     Поля **Адрес** и **Порт** для дополнительного syslog-сервера недоступны для редактирования, если снят флажок **Использовать дополнительный syslog-сервер, если основной syslog-сервер недоступен**.

     IP-адрес можно указать только в формате IPv4.

10. Нажмите на кнопку **OK**.

Настроенные параметры интеграции с SIEM будут применены.

Настройка параметров уведомлений

Чтобы настроить уведомления Kaspersky Embedded Systems Security, выполните следующие действия:

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.

2. Выберите группу администрирования, для которой требуется настроить параметры программы.

3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:

   - Чтобы настроить параметры программы для группы защищаемых устройств, выберите закладку **Политики** и откройте окно **Свойства: <Имя политики>**.

   - Чтобы настроить параметры программы для отдельного защищаемого устройства, выберите закладку **Устройства** и откройте окно **Параметры программы**.

     Если к устройству применяется активная политика Kaspersky Security Center, запрещающая изменение параметров программы, эти параметры недоступны для изменения в окне **Параметры программы**.

4. В разделе **Журналы и уведомления** в подразделе **Уведомления о событиях** нажмите на кнопку **Настройка**.

5. В окне **Настройка уведомлений** настройте следующие параметры Kaspersky Embedded Systems Security согласно вашим требованиям:

   - В списке **Настройка уведомлений** выберите тип уведомления, параметры которого вы хотите настроить.

   - В разделе **Уведомление пользователей** настройте способ уведомления пользователей. Если требуется, задайте текст уведомления.

   - В разделе **Уведомление администраторов** настройте способ уведомления администратора. Если требуется, задайте текст уведомления. Если требуется, настройте дополнительные параметры уведомлений по кнопке **Настройка**.

   - В разделе **Пороги формирования событий** укажите интервалы времени, по истечении которых Kaspersky Embedded Systems Security регистрирует события *Базы программы устарели*, *Базы программы сильно устарели* и *Проверка важных областей защищаемого устройства давно не выполнялась*.

     - **Базы программы устарели (сут)**
     - **Базы программы сильно устарели (сут)**
     - **Проверка важных областей защищаемого устройства давно не выполнялась (сут)**

6. Нажмите на кнопку **OK**.

Настроенные параметры уведомлений будут сохранены.

Настройка обмена информацией с Сервером администрирования

Чтобы выбрать типы объектов, информацию о которых Kaspersky Embedded Systems Security будет передавать на Сервер администрирования Kaspersky Security Center, выполните следующие действия:

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.

2. Выберите группу администрирования, для которой требуется настроить параметры программы.

3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:

   - Чтобы настроить параметры программы для группы защищаемых устройств, выберите закладку **Политики** и откройте окно **Свойства: <Имя политики>**.

   - Чтобы настроить параметры программы для отдельного защищаемого устройства, выберите закладку **Устройства** и откройте окно **Параметры программы**.

     Если к устройству применяется активная политика Kaspersky Security Center, запрещающая изменение параметров программы, эти параметры недоступны для изменения в окне **Параметры программы**.

4. В разделе **Журналы и уведомления** в подразделе **Взаимодействие с Сервером администрирования** нажмите на кнопку **Настройка**.

   Откроется окно **Взаимодействие с Сервером администрирования**.

5. В окне **Взаимодействие с Сервером администрирования** выберите типы объектов, информацию о которых Kaspersky Embedded Systems Security будет передавать на Сервер администрирования Kaspersky Security Center:

   - объекты на карантине;

   - резервные копии объектов.

6. Нажмите на кнопку **ОК**.

   Kaspersky Embedded Systems Security будет передавать информацию о выбранных типах объектов на Сервер администрирования.

Настройка уведомлений

Этот раздел содержит информацию о возможных способах уведомления пользователей и администраторов Kaspersky Embedded Systems Security о событиях программы и состоянии защиты устройства, а также инструкцию по настройке уведомлений.

Способы уведомления администратора и пользователей

Вы можете настроить уведомление администратора и пользователей, которые обращаются к устройству, о событиях, связанных с работой Kaspersky Embedded Systems Security, и о состоянии антивирусной защиты устройства.

Программа обеспечивает выполнение следующих задач:

- Администратор может получать информацию о событиях выбранных типов.
- Пользователи локальной сети, которые обращаются к устройству, и пользователи терминального устройства могут получать информацию о событиях типа *Обнаружен объект*, возникших в задаче Постоянная защита файлов.

В Консоли программы можно активировать уведомления администратора или пользователей несколькими способами:

- Способы уведомления пользователей:
  a. Средства службы терминалов.

     Вы можете применять этот способ для оповещения пользователей терминального защищаемого устройства, если защищаемое устройство является терминальным.

  b. Средства службы сообщений.

     Вы можете применять этот способ для оповещения через службы сообщений Microsoft Windows.

- Способы уведомления администраторов:
  a. Средства службы сообщений.

     Вы можете применять этот способ для оповещения через службы сообщений Microsoft Windows.

  b. Запуск исполняемого файла.

     При возникновении события запускается исполняемый файл, который хранится на локальном диске защищаемого устройства.

  c. Отправка по электронной почте.

     Этот способ использует для передачи сообщений электронную почту.

Вы можете составить текст сообщений для отдельных типов событий. В него вы можете включать поля с информацией о событии. По умолчанию для уведомлений пользователей используется стандартный текст сообщений.

Настройка уведомлений администратора и пользователей

Настройка уведомлений о событии предполагает выбор и настройку способа уведомлений, а также составление текста сообщения.

Чтобы настроить уведомления о событиях, выполните следующие действия:

1. В дереве Консоли программы откройте контекстное меню узла **Журналы и уведомления** и выберите пункт **Свойства**.

   Откроется окно **Параметры журналов и уведомлений**.

2. На закладке **Уведомления** выберите способ уведомления:

   a. В списке **Тип события** выберите событие, для которого вы хотите выбрать способ уведомления.

   b. В группе параметров **Уведомление администраторов** или **Уведомление пользователей** установите флажок рядом со способами уведомлений, которые вы хотите использовать.

   > Уведомление пользователя можно настроить только для следующих событий: **Обнаружен объект**, **Обнаружено и запрещено недоверенное устройство** и **Компьютер добавлен в список недоверенных**.

3. Если вы хотите составить текст сообщения, выполните следующие действия:

   a. Нажмите на кнопку **Текст сообщения**.

   b. В открывшемся окне введите текст, который будет отображаться в сообщении о событии.

   > Вы можете составить один текст сообщения для нескольких типов событий: после выбора способа уведомлений для одного типа событий, выберите остальные типы событий, для которых вы хотите использовать этот же текст сообщения, с помощью клавиш **CTRL** и **SHIFT**, а затем нажмите на кнопку **Текст сообщения**.

   a. Чтобы добавить поля с информацией о событии, нажмите на кнопку **Макрос** и выберите нужные пункты из раскрывающегося списка. Поля с информацией о событиях описаны в таблице в этом разделе.

   b. Чтобы восстановить текст сообщения, предусмотренный для события по умолчанию, нажмите на кнопку **По умолчанию**.

4. Чтобы настроить способы уведомления администраторов о выбранном событии, выберите закладку **Настройка** и в разделе **Уведомление администраторов** нажмите на кнопку **Уведомления**. Затем в окне **Дополнительные параметры** выполните настройку выбранных способов уведомления. Для этого выполните следующие действия:

   a. Для уведомлений по электронной почте выберите закладку **Электронная почта** и в соответствующих полях укажите адреса электронной почты получателей (разделяйте адреса точкой с запятой), имя или сетевой адрес SMTP-сервера и номер порта. Если требуется, укажите текст, который будет отображаться в полях **Тема** и **От**. В текст поля **Тема** можно также добавлять переменные с информацией о событии (см. таблицу ниже).

      Если вы хотите использовать проверку подлинности по учетной записи при соединении с SMTP-сервером, в группе **Параметры аутентификации** установите флажок **Использовать SMTP-аутентификацию** и укажите имя и пароль пользователя, учетная запись которого будет проверяться.

   b. Для уведомлений средствами службы сообщений Windows составьте список защищаемых устройств, получающих уведомления, на закладке **Служба сообщений**: для каждого защищаемого устройства,

которое вы хотите добавить, нажмите на кнопку **Добавить** и в поле ввода введите его сетевое имя.

c. Для запуска исполняемого файла на закладке **Исполняемый файл** выберите файл на локальном диске защищаемого устройства или введите полный путь к нему. Этот файл будет выполняться на защищаемом устройстве при возникновении события. Введите имя и пароль пользователя, под учетной записью которого файл будет выполняться.

Указывая путь к исполняемому файлу, вы можете использовать системные переменные окружения; вы не можете использовать пользовательские переменные окружения.

Если вы хотите ограничить количество уведомлений о событиях одного типа за период времени, на закладке **Дополнительно** установите флажок **Не отправлять одно и то же уведомление чаще** и укажите количество экземпляров и период времени.

5. Нажмите на кнопку **ОК**.

Настроенные параметры уведомлений будут сохранены.

Поля с информацией о событии

Переменная	Описание
%EVENT_TYPE%	Тип события.
%EVENT_TIME%	Время возникновения события.
%EVENT_SEVERITY%	Уровень важности события.
%OBJECT%	Имя объекта (в задачах постоянной защиты компьютера и проверки по требованию). В задаче Обновление модулей программы включает название обновления и адрес страницы в интернете с информацией об обновлении.
%VIRUS_NAME%	Имя объекта согласно классификации Вирусной энциклопедии. Это имя входит в полное название обнаруженного объекта, которое Kaspersky Embedded Systems Security возвращает при обнаружении объекта. Вы можете просмотреть полное название обнаруженного объекта в журнале выполнения задачи.
%VIRUS_TYPE%	Тип обнаруженного объекта по классификации "Лаборатории Касперского", например, "вирус" или "троянская программа". Входит в полное название обнаруженного объекта, которое Kaspersky Embedded Systems Security возвращает, признав объект зараженным или возможно зараженным. Вы можете просмотреть полное название обнаруженного объекта в журнале выполнения задачи.
%USER_COMPUTER%	В задаче Постоянная защита файлов имя защищаемого устройства пользователя, который обратился к объекту на устройстве.
%USER_NAME%	В задаче Постоянная защита файлов имя пользователя, который обратился к объекту на устройстве.
%FROM_COMPUTER%	Имя защищаемого устройства, с которого поступило уведомление.
%EVENT_REASON%	Причина возникновения события (некоторые события не имеют этого поля).
%ERROR_CODE%	Код ошибки (только для события "внутренняя ошибка задачи").
%TASK_NAME%	Название задачи (имеется только у событий, связанных с выполнением задач).

Запуск и остановка Kaspersky Embedded Systems Security

Этот раздел содержит информацию о запуске Консоли программы, а также о запуске и остановке службы Kaspersky Security.

Запуск Плагина управления Kaspersky Embedded Systems Security

Для запуска Плагина управления Kaspersky Embedded Systems Security в Kaspersky Security Center дополнительных действий не требуется. После установки Плагина управления на защищаемое устройство администратора, он запускается вместе с Kaspersky Security Center. Подробная информация о запуске Kaspersky Security Center приведена в *Справке Kaspersky Security Center*.

Запуск Консоли Kaspersky Embedded Systems Security из меню Пуск

Названия параметров могут отличаться в разных операционных системах Windows.

*Чтобы запустить Консоль программы из меню **Пуск**, выполните следующие действия:*

1. В меню **Пуск** выберите **Программы** > **Kaspersky Embedded Systems Security** > **Средства администрирования** > **Консоль Kaspersky Embedded Systems Security**.

Чтобы добавить в Консоль программы другие оснастки, запустите Консоль программы в авторском режиме.

Чтобы запустить Консоль программы в авторском режиме, выполните следующие действия:

1. В меню **Пуск** выберите **Программы** > **Kaspersky Embedded Systems Security** > **Средства администрирования**.
2. В контекстном меню Консоли программы выберите команду **Автор**.

   Консоль программы будет запущена в авторском режиме.

При запуске Консоли программы на защищаемом устройстве откроется окно Консоли программы.

Если вы запустили Консоль программы не на защищаемом устройстве, подключитесь к защищаемому устройству.

Чтобы подключиться к защищаемому устройству, выполните следующие действия:

1. В дереве Консоли программы откройте контекстное меню узла **Kaspersky Embedded Systems Security**.
2. Выберите команду **Подключиться к другому компьютеру**.

   Откроется окно **Выбор сервера**.
3. В открывшемся окне выберите **Другой сервер**.
4. В поле ввода справа укажите сетевое имя защищаемого устройства.
5. Нажмите на кнопку **OK**.

Консоль программы подключится к защищаемому устройству.

Если учетная запись, используемая для входа в Microsoft Windows, не обладает правами доступа к службе Kaspersky Security Management на защищаемом устройстве, установите флажок **Установить соединение с правами учетной записи** и укажите другую учетную запись, которая обладает такими правами.

Запуск и остановка службы Kaspersky Security

По умолчанию служба Kaspersky Security запускается автоматически сразу после операционной системы. Служба Kaspersky Security управляет рабочими процессами, в которых выполняются задачи постоянной защиты компьютера, контроля компьютера, проверки по требованию и обновления.

По умолчанию при запуске Kaspersky Embedded Systems Security запускаются задачи Постоянная защита файлов и Проверка при старте операционной системы, а также другие задачи, в расписании которых указана частота запуска **При запуске программы**.

Если вы остановите службу Kaspersky Security, все выполняющиеся задачи будут остановлены. После того как вы снова запустите службу Kaspersky Security, программа автоматически запустит только задачи, в расписании которых указано **При запуске программы**. Остальные задачи нужно запустить вручную.

Вы можете запускать и останавливать службу Kaspersky Security с помощью контекстного меню узла **Kaspersky Embedded Systems Security** или с помощью оснастки Службы Microsoft Windows.

Вы можете запускать и останавливать Kaspersky Embedded Systems Security, если вы входите в группу администраторов на защищаемом устройстве.

Чтобы остановить или запустить программу с помощью Консоли программы, выполните следующие действия:

1. В дереве Консоли программы откройте контекстное меню узла **Kaspersky Embedded Systems Security**.
2. Выберите одну из следующих команд:
   - **Остановить программу**
   - **Запустить программу**

   Служба Kaspersky Security будет запущена или остановлена.

Запуск компонентов Kaspersky Embedded Systems Security при безопасном режиме загрузки операционной системы

В этом разделе приведена информация о работе Kaspersky Embedded Systems Security при безопасном режиме загрузки операционной системы.

О работе Kaspersky Embedded Systems Security при безопасном режиме загрузки операционной системы

Компоненты Kaspersky Embedded Systems Security можно запустить при загрузке операционной системы в безопасном режиме. Наряду со службой Kaspersky Security (kavfs.exe) загружается драйвер klam.sys. Драйвер используется для регистрации службы Kaspersky Security как защищенной службы при загрузке операционной системы. Дополнительные сведения приведены в разделе Регистрация службы Kaspersky Security как защищенной службы.

Kaspersky Embedded Systems Security можно запустить при загрузке операционной системы в следующих безопасных режимах:

- Безопасный режим с типом загрузки "Минимальная" – стандартный вариант безопасного режима загрузки операционной системы. При этом Kaspersky Embedded Systems Security может запускать следующие компоненты:
  - Постоянная защита файлов.
  - Проверка по требованию.
  - Контроль запуска программ и Формирование правил контроля запуска программ.
  - Анализ журналов.
  - Мониторинг файловых операций.
  - Мониторинг целостности файлов на основе эталона.
  - Проверка целостности программы.

Безопасный режим с типом загрузки "Сеть" – загрузка операционной системы в безопасном режиме с поддержкой сетевых драйверов. В этом режиме помимо компонентов, запускаемых в безопасном режиме с типом загрузки "Минимальная", Kaspersky Embedded Systems Security может запускать следующие компоненты:

- Обновление баз программы.
- Обновление модулей программы.

Запуск Kaspersky Embedded Systems Security в безопасном режиме

По умолчанию Kaspersky Embedded Systems Security не запускается при загрузке операционной системы в безопасном режиме.

Чтобы запустить Kaspersky Embedded Systems Security при безопасном режиме загрузки операционной системы, выполните следующие действия:

1. Запустите редактор реестра Windows (C:\Windows\regedit.exe).
2. В системном реестре откройте ключ [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\klam\Parameters].
3. Откройте параметр LoadInSafeMode.
4. Установите для него значение `1`.
5. Нажмите на кнопку **OK**.

Чтобы отменить запуск Kaspersky Embedded Systems Security при безопасном режиме загрузки операционной системы, выполните следующие действия:

1. Запустите редактор реестра Windows (C:\Windows\regedit.exe).
2. В системном реестре откройте ключ [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\klam\Parameters].
3. Откройте параметр LoadInSafeMode.
4. Установите для него значение `0`.
5. Нажмите на кнопку **OK**.

Механизмы самозащиты Kaspersky Embedded Systems Security

Этот раздел содержит информацию о механизмах самозащиты Kaspersky Embedded Systems Security.

О механизмах самозащиты Kaspersky Embedded Systems Security

В Kaspersky Embedded Systems Security реализованы механизмы самозащиты, обеспечивающие защиту от изменения или удаления папок программы, процессов памяти и записей системного реестра.

Защита от изменений папок с установленными компонентами Kaspersky Embedded Systems Security

Kaspersky Embedded Systems Security запрещает всем пользователям переименовывать и удалять папки с установленными компонентами программы. По умолчанию используются следующие пути к папкам установки программы:

- В 32-х разрядной версии Microsoft Windows: %ProgramFiles%\Kaspersky Lab\Kaspersky Embedded Systems Security\
- В 64-х разрядной версии Microsoft Windows: %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Embedded Systems Security\

Защита от изменений ключей реестра Kaspersky Embedded Systems Security

Kaspersky Embedded Systems Security ограничивает доступ к следующим ключам и ветвям реестра, обеспечивающим загрузку драйверов и служб программы:

- [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\ESS]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\kavfs]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\kavfsgt]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\kavfsslp]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\klam]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\klelaml]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\klfltdev]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\klramdisk]
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\ESS\3.0\CrashDump]
- [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\ESS\3.0\CrashDump] (в 64-разрядной версии Microsoft Windows)

- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\ESS\2.3\Trace]
- [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\ESS\3.0\Trace] (в 64-разрядной версии Microsoft Windows)

Права на изменение этих ветвей и ключей реестра имеют только пользователи с учетной записью Локальная система (SYSTEM). Пользователи с учетными записями Пользователь и Администратор имеют права только на чтение.

Регистрация службы Kaspersky Security как защищенной службы

Технология *Protected Process Light* (PPL) гарантирует, что операционная система выполняет загрузку только доверенных служб и процессов. Для того чтобы запустить службу как защищенную, на защищаемом устройстве должен быть установлен драйвер *Early Launch Antimalware*.

Драйвер *Early Launch Antimalware* (ELAM) обеспечивает защиту устройств в сети при их включении и при инициализации драйверов сторонних производителей.

Драйвер ELAM устанавливается автоматически во время установки Kaspersky Embedded Systems Security и используется для регистрации службы Kaspersky Security как защищенной во время запуска операционной системы. Когда служба Kaspersky Security (KAVFS) запускается как системный защищенный процесс, другие незащищенные процессы в системе не могут внедрять потоки, записывать в виртуальную память защищенного процесса и останавливать службу.

При запуске процесса как защищенного пользователь не может управлять им, независимо от прав пользователя. Регистрация службы Kaspersky Security как защищенной с помощью драйвера ELAM поддерживается операционной системой Microsoft Windows 10 и более поздними версиями. Если программа Kaspersky Embedded Systems Security установлена на сервер под управлением операционной системы, поддерживающей PPL, управление правами пользователей для службы Kaspersky Security (KAVFS) будет недоступно.

Чтобы установить Kaspersky Embedded Systems Security как защищенный процесс, выполните следующую команду:

```
msiexec /i ess_x64.msi NOPPL=0 EULA=1 PRIVACYPOLICY=1 /qn
```

Управление правами доступа к функциям Kaspersky Embedded Systems Security

Этот раздел содержит информацию о правах на управление Kaspersky Embedded Systems Security и службами операционной системы, которые регистрирует программа, а также инструкции по настройке этих прав.

О правах на управление Kaspersky Embedded Systems Security

По умолчанию доступ ко всем функциям Kaspersky Embedded Systems Security имеют пользователи, входящие в группу Администраторы на защищаемом устройстве, пользователи группы ESS Administrators, созданной на защищаемом устройстве при установке Kaspersky Embedded Systems Security, а также группа SYSTEM.

Пользователи, которые имеют доступ уровня Изменение прав в Kaspersky Embedded Systems Security, могут предоставлять доступ к функциям Kaspersky Embedded Systems Security другим пользователям, зарегистрированным на защищаемом устройстве или входящим в домен.

Пользователи, не зарегистрированные в списке пользователей Kaspersky Embedded Systems Security, не могут открыть Консоль программы.

Вы можете выбрать для пользователя или группы пользователей один из следующих стандартных уровней доступа:

- **Полный контроль** – доступ ко всем функциям программы: возможность просматривать и изменять общие параметры Kaspersky Embedded Systems Security, параметры компонентов и права пользователей Kaspersky Embedded Systems Security, а также возможность просматривать статистику Kaspersky Embedded Systems Security.

- **Изменение** – доступ ко всем функциям программы, за исключением изменения прав пользователей: возможность просматривать и изменять общие параметры Kaspersky Embedded Systems Security и параметры компонентов Kaspersky Embedded Systems Security.

- **Чтение** – возможность просматривать общие параметры Kaspersky Embedded Systems Security, параметры компонентов Kaspersky Embedded Systems Security, статистику Kaspersky Embedded Systems Security и права пользователей Kaspersky Embedded Systems Security.

Вы также можете настроить расширенные права доступа: разрешить или запретить доступ к конкретным функциям Kaspersky Embedded Systems Security.

Если вы вручную настроили права доступа для пользователя или группы, то для этого пользователя или группы будет установлен уровень доступа **Особые разрешения**.

Права доступа к функциям Kaspersky Embedded Systems Security

Права доступа	Описание
Управление задачами	Возможность запускать / останавливать / приостанавливать / возобновлять задачи Kaspersky Embedded Systems Security.
Создание и удаление задач проверки по требованию	Возможность создавать и удалять задачи проверки по требованию.
Изменение параметров	Возможности: • Импортировать параметры Kaspersky Embedded Systems Security из конфигурационного файла. • Редактировать настройки программы.
Чтение параметров	Возможности: • Просматривать общие параметры Kaspersky Embedded Systems Security и параметры задач. • Экспортировать параметры Kaspersky Embedded Systems Security в конфигурационный файл. • Просматривать параметры журналов выполнения задач, журнала системного аудита и уведомлений.
Управление хранилищами	Возможности: • Помещать объекты на карантин.

	• Удалять объекты из карантина и резервного хранилища. • Восстанавливать объекты из карантина и резервного хранилища.
Управление журналами	Возможность удалять журналы выполнения задач и очищать журнал системного аудита.
Чтение журналов	Возможность просматривать события в журналах выполнения задач и журнале системного аудита.
Чтение статистики	Возможность просматривать статистику работы каждой задачи Kaspersky Embedded Systems Security.
Лицензирование программы	Возможность активировать Kaspersky Embedded Systems Security.
Удаление программы	Возможность удалить Kaspersky Embedded Systems Security.
Чтение прав	Возможность просматривать список и права доступа пользователей Kaspersky Embedded Systems Security.
Изменение прав	Возможности: • Изменять список пользователей, имеющих доступ к управлению программой. • Изменять права доступа пользователей к функциям Kaspersky Embedded Systems Security.

О правах на управление регистрируемыми службами

При установке Kaspersky Embedded Systems Security регистрирует в Windows службу Kaspersky Security (KAVFS), службу Kaspersky Security Management (KAVFSGT) и службу Kaspersky Security Exploit Prevention (KAVFSSLP).

Регистрация службы Kaspersky Security как защищенной с помощью драйвера ELAM поддерживается операционной системой Microsoft Windows 10 и более поздних версий. При запуске процесса как защищенного пользователь не может управлять им, независимо от прав пользователя. Если программа Kaspersky Embedded Systems Security установлена на защищаемом устройстве с операционной системой, поддерживающей PPL, управление правами для службы Kaspersky Security (KAVFS) будет недоступно.

Служба Kaspersky Security

По умолчанию доступ к управлению службой Kaspersky Security имеют пользователи, входящие в группу "Администраторы" на защищаемом устройстве, а также системные группы SERVICE и INTERACTIVE с правами на чтение и системная группа SYSTEM с правами на чтение и исполнение.

Пользователи, имеющие доступ уровня Изменение прав, могут предоставлять права на управление службой Kaspersky Security другим пользователям, зарегистрированным на защищаемом устройстве или входящим в домен.

Служба Kaspersky Security Management

Для управления программой через Консоль программы, установленную на другом защищаемом устройстве, требуется, чтобы учетная запись, с правами которой происходит подключение к Kaspersky Embedded Systems Security, имела полный доступ к службе Kaspersky Security Management на защищаемом устройстве.

По умолчанию доступ к службе Kaspersky Security Management имеют пользователи, входящие в группу Администраторы на защищаемом устройстве, и пользователи группы ESS Administrators, созданной на защищаемом устройстве при установке Kaspersky Embedded Systems Security.

Вы можете управлять службой Kaspersky Security Management только через оснастку Службы Microsoft Windows.

Служба Kaspersky Security Exploit Prevention

По умолчанию доступ к управлению службой Kaspersky Security Exploit Prevention имеют пользователи, входящие в группу "Администраторы" на защищаемом устройстве, а также в группу SYSTEM с правами на чтение и исполнение.

О правах доступа к службе Kaspersky Security Management

Вы можете просмотреть список служб Kaspersky Embedded Systems Security.

При установке Kaspersky Embedded Systems Security регистрирует службу Kaspersky Security Management (KAVFSGT). Для управления программой через Консоль программы, установленную на другом защищаемом устройстве, требуется, чтобы учетная запись, используемая для подключения к Kaspersky Embedded Systems Security, имела полный доступ к службе Kaspersky Security Management на защищаемом устройстве.

По умолчанию доступ к службе Kaspersky Security Management имеют пользователи, входящие в группу Администраторы на защищаемом устройстве, и пользователи группы ESS Administrators, созданной на защищаемом устройстве при установке Kaspersky Embedded Systems Security.

Вы можете управлять службой Kaspersky Security Management только через оснастку Службы Microsoft Windows.

Нельзя разрешить или запретить пользователям доступ к службе Kaspersky Security Management при настройке параметров Kaspersky Embedded Systems Security.

Вы можете подключиться к Kaspersky Embedded Systems Security с локальной учетной записью, если на защищаемом устройстве зарегистрирована учетная запись с таким же именем пользователя и паролем.

О правах на управление службой Kaspersky Security

При установке Kaspersky Embedded Systems Security регистрирует в Windows службу Kaspersky Security (KAVFS), а также включает функциональные компоненты, запускаемые при запуске операционной системы. Чтобы снизить риск стороннего доступа к функциям программы и параметрам безопасности защищаемого устройства с помощью службы Kaspersky Security, можно ограничить права на управление службой Kaspersky Security с помощью Консоли программы или Плагина управления.

По умолчанию доступ к управлению службой Kaspersky Security имеют пользователи, входящие в группу Администраторы на защищаемом устройстве. Права на чтение имеют группы SERVICE и INTERACTIVE, а права на чтение и исполнение имеет группа SYSTEM.

Вы не можете удалить учетную запись пользователя SYSTEM или изменять права этой учетной записи. Если права учетной записи SYSTEM были изменены, то при сохранении изменений для этой учетной записи восстанавливаются максимальные права.

Пользователи, имеющие доступ к функциям уровня Изменение прав, могут предоставлять права на управление службой Kaspersky Security другим пользователям, зарегистрированным на защищаемом устройстве или входящим в домен.

Вы можете выбрать для пользователя или группы пользователей Kaspersky Embedded Systems Security один из следующих стандартных уровней доступа для управления службой Kaspersky Security:

- **Полный контроль** – возможность просматривать и изменять общие параметры работы и права пользователей для службы Kaspersky Security, а также запускать и останавливать службу Kaspersky Security.
- **Чтение** – возможность просматривать общие параметры и права пользователей для службы Kaspersky Security.
- **Изменение** – возможность просматривать и изменять общие параметры работы и права пользователей для службы Kaspersky Security.
- **Исполнение** – возможность запускать и останавливать службу Kaspersky Security.

Также вы можете выполнять расширенную настройку прав доступа: разрешить или запретить доступ к определенным функциям Kaspersky Embedded Systems Security (см. таблицу ниже).

Если вы вручную настроили права доступа для пользователя или группы, то для этого пользователя или группы будет установлен уровень доступа **Особые разрешения**.

Права доступа к функциям службы Kaspersky Security

Функция	Описание
Просмотр параметров службы	Возможность просматривать общие параметры и права пользователей для службы Kaspersky Security.
Запрос статуса службы у Диспетчера управления службами	Возможность запрашивать статус выполнения службы Kaspersky Security у Диспетчера управления службами Microsoft Windows.
Запрос статуса у службы	Возможность запрашивать статус выполнения службы у Kaspersky Security.
Перечисление зависимых служб	Возможность просматривать список служб, от которых зависит служба Kaspersky Security, а также служб, зависимых от службы Kaspersky Security.
Изменение параметров службы	Возможность просматривать и изменять общие параметры работы и права пользователей для служб Kaspersky Security.
Запуск службы	Возможность запускать выполнение службы Kaspersky Security.
Остановка службы	Возможность останавливать выполнение службы Kaspersky Security.
Приостановка / Возобновление службы	Возможность приостанавливать и возобновлять выполнение службы Kaspersky Security.

Чтение прав	Возможность просматривать список пользователей службы Kaspersky Security и права доступа каждого пользователя.
Изменение прав	Возможности: • добавлять и удалять пользователей службы Kaspersky Security; • изменять права доступа пользователей к службе Kaspersky Security.
Удаление службы	Возможность отмены регистрации службы Kaspersky Security в диспетчере управления службами Microsoft Windows.
Пользовательские запросы к службе	Возможность создавать и отправлять пользовательские запросы к службе Kaspersky Security.

Управление правами доступа с помощью Плагина управления

В этом разделе описана навигация в интерфейсе Плагина управления и настройка прав доступа для одного или всех защищаемых устройств сети.

Настройка прав доступа к Kaspersky Embedded Systems Security и службе Kaspersky Security

Можно настраивать список пользователей и групп пользователей, которым разрешен доступ к функциям Kaspersky Embedded Systems Security и к управлению службой Kaspersky Security. Можно также настраивать права доступа для этих пользователей и групп пользователей.

Чтобы добавить в список или удалить из списка пользователя или группу, выполните следующие действия:

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить параметры программы.
3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
   - Чтобы настроить параметры программы для группы защищаемых устройств, выберите закладку **Политики** и откройте окно **Свойства: <Имя политики>**.
   - Чтобы настроить параметры программы для отдельного защищаемого устройства, выберите закладку **Устройства** и откройте окно **Параметры программы**.

     Если к устройству применяется активная политика Kaspersky Security Center, запрещающая изменение параметров программы, эти параметры недоступны для изменения в окне **Параметры программы**.
4. В разделе **Дополнительные возможности** выполните одно из следующих действий:

- Нажмите на кнопку **Настройка** в подразделе **Права пользователей на управление программой**, если вы хотите изменить список пользователей, которые имеют доступ к управлению функциями Kaspersky Embedded Systems Security.

- Нажмите на кнопку **Настройка** в подразделе **Права пользователей на управление службой Kaspersky Security**, если вы хотите изменить список пользователей, которые имеют доступ на управление службой Kaspersky Security.

  Откроется окно **Разрешения для Kaspersky Embedded Systems Security 3**.

5. В открывшемся окне выполните следующие действия:

   - Чтобы добавить пользователя или группу в список, нажмите на кнопку **Добавить** и выберите пользователя или группу, которым вы хотите предоставить права.

   - Чтобы удалить пользователя или группу из списка, выберите пользователя или группу, доступ для которых вы хотите ограничить, и нажмите на кнопку **Удалить**.

6. Нажмите на кнопку **Применить**.

Выбранные пользователи (группы) будут добавлены или удалены.

Чтобы изменить права пользователя или группы на управление Kaspersky Embedded Systems Security или службой Kaspersky Security, выполните следующие действия:

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.

2. Выберите группу администрирования, для которой требуется настроить параметры программы.

3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:

   - Чтобы настроить параметры программы для группы защищаемых устройств, выберите закладку **Политики** и откройте окно **Свойства: <Имя политики>**.

   - Чтобы настроить параметры программы для отдельного защищаемого устройства, выберите закладку **Устройства** и откройте окно **Параметры программы**.

     Если к устройству применяется активная политика Kaspersky Security Center, запрещающая изменение параметров программы, эти параметры недоступны для изменения в окне **Параметры программы**.

4. В разделе **Дополнительные возможности** выполните одно из следующих действий:

   - Нажмите на кнопку **Настройка** в подразделе **Права пользователей на управление программой**, если вы хотите изменить список пользователей, которые имеют доступ к управлению функциями Kaspersky Embedded Systems Security.

   - Нажмите на кнопку **Настройка** в подразделе **Права пользователей на управление службой Kaspersky Security**, если вы хотите изменить список пользователей, которые имеют доступ к управлению программой с помощью службы Kaspersky Security.

     Откроется окно **Разрешения для Kaspersky Embedded Systems Security**.

5. В открывшемся окне в списке **Имена групп и пользователей** выберите пользователя или группу пользователей, права которых вы хотите изменить.

6. В блоке **Разрешения для <Пользователь (Группа)>** установите флажки **Разрешить** или **Запретить** для следующих уровней доступа:

   - **Полный контроль**: полный набор прав на управление Kaspersky Embedded Systems Security или службой Kaspersky Security.
   - **Чтение**:
     - Следующие разрешения на управление Kaspersky Embedded Systems Security: **Чтение статистики**, **Чтение параметров**, **Чтение журналов**, **Чтение прав**.
     - Следующие разрешения на управление службой Kaspersky Security: **Чтение параметров службы**, **Запрос статуса службы у Диспетчера управления службами**, **Запрос статуса у службы**, **Чтение списка зависимых служб**, **Чтение прав**.
   - **Изменение**:
     - Все права на управление Kaspersky Embedded Systems Security, кроме **Изменение прав**.
     - Следующие права на управление службой Kaspersky Security: **Чтение прав**, **Настройка параметров службы**.
   - **Особые разрешения**: следующие разрешения на управление службой Kaspersky Security: **Запуск KAVFS**, **Остановка KAVFS**, **Приостановка / Возобновление KAVFS**, **Чтение прав**, **Пользовательские запросы к KAVFS**.

7. Чтобы выполнить расширенную настройку прав для пользователя или группы (**Особые разрешения**), нажмите на кнопку **Дополнительно**.

   a. В открывшемся окне **Дополнительные параметры безопасности для службы Kaspersky Embedded Systems Security** выберите нужного пользователя или группу.

   b. Нажмите на кнопку **Изменить**.

   c. В раскрывающемся списке в верхней части окна выберите тип контроля доступа: **Разрешить** или **Запретить**.

   d. Установите флажки напротив тех функций, которые вы хотите разрешить или запретить выбранному пользователю или выбранной группе.

   e. Нажмите на кнопку **OK**.

   f. В окне **Дополнительные параметры безопасности для службы Kaspersky Embedded Systems Security** нажмите на кнопку **OK**.

8. В окне **Разрешения для службы Kaspersky Embedded Systems Security** нажмите на кнопку **Применить**.

Настроенные права на управление Kaspersky Embedded Systems Security или службой Kaspersky Security будут сохранены.

Защита доступа к функциям Kaspersky Embedded Systems Security с помощью пароля

Настройка прав пользователей позволяет ограничивать доступ к управлению программой и регистрируемыми службами. Для дополнительной защиты критических операций можно также установить защиту паролем в параметрах Kaspersky Embedded Systems Security.

Kaspersky Embedded Systems Security запрашивает ввод пароля при попытке доступа к следующим функциям программы:

- подключение к Консоли программы;
- удаление Kaspersky Embedded Systems Security;
- изменение состава компонентов Kaspersky Embedded Systems Security;
- выполнение команд командной строки.

Интерфейс Kaspersky Embedded Systems Security скрывает вводимый пароль на экране. Kaspersky Embedded Systems Security хранит пароль в виде контрольной суммы, рассчитываемой при вводе пароля.

Kaspersky Embedded Systems Security не проверяет надежность пароля и не блокирует ввод пароля после нескольких неудачных попыток.

При создании пароля рекомендуется выполнить следующие условия:

- Пароль не должен содержать имя учетной записи и имя компьютера.
- Длина пароля должна составлять не менее 8 символов.
- Пароль должен содержать символы, принадлежащие как минимум к трем из следующих категорий:
  - заглавные латинские буквы (A-Z);
  - строчные латинские буквы (a-z);
  - цифры (0-9);
  - символы: восклицательный знак (!), значок доллара ($), значок решетки (#) и значок процента (%).

Можно импортировать и экспортировать конфигурацию программ, защищенных паролем. Конфигурационный файл, созданный при экспорте конфигурации защищенной программы, содержит контрольную сумму пароля и значение модификатора, используемого для заполнения строки пароля.

Не изменяйте контрольную сумму и модификатор в конфигурационном файле. Импорт защищенной паролем конфигурации, измененной вручную, может вызвать полную блокировку доступа к программе.

Чтобы защитить доступ к функциям Kaspersky Embedded Systems Security, выполните следующие действия:

1. В дереве Консоли администрирования Kaspersky Security Center разверните узел **Управляемые устройства**. Выберите группу администрирования, содержащую защищаемые устройства, для которых вы хотите настроить параметры программы.
2. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
   - Чтобы настроить параметры политики для группы защищаемых устройств, выберите закладку **Политики** и с помощью контекстного меню перейдите к свойствам **<Имя политики>**.

- Чтобы настроить параметры программы для отдельного защищаемого устройства, откройте окно **Параметры программы** в Kaspersky Security Center.

3. На закладке **Параметры программы** в разделе **Безопасность** нажмите на кнопку **Настройка**.

   Откроется окно **Параметры безопасности**.

4. В разделе **Параметры применения пароля** установите флажок **Использовать защиту паролем**.

   Поля **Пароль** и **Подтверждение пароля** станут активными.

5. В поле **Пароль** введите пароль, который вы хотите использовать для защиты доступа к функциям Kaspersky Embedded Systems Security.

6. В поле **Подтверждение пароля** введите пароль повторно.

7. Нажмите на кнопку **OK**.

Настроенные параметры будут сохранены. Kaspersky Embedded Systems Security будет запрашивать указанный пароль для доступа к защищенным функциям.

Установленный пароль невозможно восстановить. Потеря пароля приведет к полной потере контроля над программой. Кроме того, невозможно будет удалить программу с защищаемого устройства.

Сбросить пароль можно в любой момент. Для этого снимите флажок **Использовать защиту паролем** и сохраните изменения. Защита паролем будет выключена, и контрольная сумма старого пароля будет удалена. Повторите процесс создания для нового пароля.

Управление правами доступа с помощью Консоли программы

В этом разделе описана навигация в интерфейсе Консоли программы и настройка прав доступа для защищаемого устройства.

Настройка прав доступа на управление Kaspersky Embedded Systems Security и службой Kaspersky Security

Можно настраивать список пользователей и групп пользователей, которым разрешен доступ к функциям Kaspersky Embedded Systems Security и к управлению службой Kaspersky Security. Можно также настраивать права доступа для этих пользователей и групп пользователей.

Чтобы добавить в список или удалить из списка пользователя или группу, выполните следующие действия:

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.

2. Выберите группу администрирования, для которой требуется настроить параметры программы.

3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:

   - Чтобы настроить параметры программы для группы защищаемых устройств, выберите закладку **Политики** и откройте окно **Свойства: <Имя политики>**.

- Чтобы настроить параметры программы для отдельного защищаемого устройства, выберите закладку **Устройства** и откройте окно **Параметры программы**.

  Если к устройству применяется активная политика Kaspersky Security Center, запрещающая изменение параметров программы, эти параметры недоступны для изменения в окне **Параметры программы**.

4. В разделе **Дополнительные возможности** выполните одно из следующих действий:

   - Нажмите на кнопку **Настройка** в подразделе **Права пользователей на управление программой**, если вы хотите изменить список пользователей, которые имеют доступ к управлению функциями Kaspersky Embedded Systems Security.

   - Нажмите на кнопку **Настройка** в подразделе **Права пользователей на управление службой Kaspersky Security**, если вы хотите изменить список пользователей, которые имеют доступ на управление службой Kaspersky Security.

     Откроется окно **Разрешения для Kaspersky Embedded Systems Security 3**.

5. В открывшемся окне выполните следующие действия:

   - Чтобы добавить пользователя или группу в список, нажмите на кнопку **Добавить** и выберите пользователя или группу, которым вы хотите предоставить права.

   - Чтобы удалить пользователя или группу из списка, выберите пользователя или группу, доступ для которых вы хотите ограничить, и нажмите на кнопку **Удалить**.

6. Нажмите на кнопку **Применить**.

Выбранные пользователи (группы) будут добавлены или удалены.

Чтобы изменить права пользователя или группы на управление Kaspersky Embedded Systems Security или службой Kaspersky Security, выполните следующие действия:

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.

2. Выберите группу администрирования, для которой требуется настроить параметры программы.

3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:

   - Чтобы настроить параметры программы для группы защищаемых устройств, выберите закладку **Политики** и откройте окно **Свойства: <Имя политики>**.

   - Чтобы настроить параметры программы для отдельного защищаемого устройства, выберите закладку **Устройства** и откройте окно **Параметры программы**.

     Если к устройству применяется активная политика Kaspersky Security Center, запрещающая изменение параметров программы, эти параметры недоступны для изменения в окне **Параметры программы**.

4. В разделе **Дополнительные возможности** выполните одно из следующих действий:

- Нажмите на кнопку **Настройка** в подразделе **Права пользователей на управление программой**, если вы хотите изменить список пользователей, которые имеют доступ к управлению функциями Kaspersky Embedded Systems Security.

- Нажмите на кнопку **Настройка** в подразделе **Права пользователей на управление службой Kaspersky Security**, если вы хотите изменить список пользователей, которые имеют доступ к управлению программой с помощью службы Kaspersky Security.

  Откроется окно **Разрешения для Kaspersky Embedded Systems Security**.

5. В открывшемся окне в списке **Имена групп и пользователей** выберите пользователя или группу пользователей, права которых вы хотите изменить.

6. В блоке **Разрешения для <Пользователь (Группа)>** установите флажки **Разрешить** или **Запретить** для следующих уровней доступа:

   - **Полный контроль**: полный набор прав на управление Kaspersky Embedded Systems Security или службой Kaspersky Security.

   - **Чтение**:

     - Следующие разрешения на управление Kaspersky Embedded Systems Security: **Чтение статистики**, **Чтение параметров**, **Чтение журналов**, **Чтение прав**.

     - Следующие разрешения на управление службой Kaspersky Security: **Чтение параметров службы**, **Запрос статуса службы у Диспетчера управления службами**, **Запрос статуса у службы**, **Чтение списка зависимых служб**, **Чтение прав**.

   - **Изменение**:

     - Все права на управление Kaspersky Embedded Systems Security, кроме **Изменение прав**.

     - Следующие права на управление службой Kaspersky Security: **Чтение прав**, **Настройка параметров службы**.

   - **Особые разрешения**: следующие разрешения на управление службой Kaspersky Security: **Запуск KAVFS**, **Остановка KAVFS**, **Приостановка / Возобновление KAVFS**, **Чтение прав**, **Пользовательские запросы к KAVFS**.

7. Чтобы выполнить расширенную настройку прав для пользователя или группы (**Особые разрешения**), нажмите на кнопку **Дополнительно**.

   a. В открывшемся окне **Дополнительные параметры безопасности для службы Kaspersky Embedded Systems Security** выберите нужного пользователя или группу.

   b. Нажмите на кнопку **Изменить**.

   c. В раскрывающемся списке в верхней части окна выберите тип контроля доступа: **Разрешить** или **Запретить**.

   d. Установите флажки напротив тех функций, которые вы хотите разрешить или запретить выбранному пользователю или выбранной группе.

   e. Нажмите на кнопку **OK**.

   f. В окне **Дополнительные параметры безопасности для службы Kaspersky Embedded Systems Security** нажмите на кнопку **OK**.

8. В окне **Разрешения для службы Kaspersky Embedded Systems Security** нажмите на кнопку **Применить**.

9. Настроенные права на управление Kaspersky Embedded Systems Security или службой Kaspersky Security будут сохранены.

Защита доступа к функциям Kaspersky Embedded Systems Security с помощью пароля

Настройка прав пользователей позволяет ограничивать доступ к управлению программой и регистрируемыми службами. Для дополнительной защиты критических операций можно также установить защиту паролем в параметрах Kaspersky Embedded Systems Security.

Kaspersky Embedded Systems Security запрашивает ввод пароля при попытке доступа к следующим функциям программы:

- подключение к Консоли программы;
- удаление Kaspersky Embedded Systems Security;
- изменение состава компонентов Kaspersky Embedded Systems Security;
- выполнение команд командной строки.

Интерфейс Kaspersky Embedded Systems Security скрывает вводимый пароль на экране. Kaspersky Embedded Systems Security хранит пароль в виде контрольной суммы, рассчитываемой при вводе пароля.

Можно импортировать и экспортировать конфигурацию программ, защищенных паролем. Конфигурационный файл, созданный при экспорте конфигурации защищенной программы, содержит контрольную сумму пароля и значение модификатора, используемого для заполнения строки пароля.

Не изменяйте контрольную сумму и модификатор в конфигурационном файле. Импорт защищенной паролем конфигурации, измененной вручную, может вызвать полную блокировку доступа к программе.

Чтобы защитить доступ к функциям Kaspersky Embedded Systems Security, выполните следующие действия:

1. В дереве Консоли программы выберите узел **Kaspersky Embedded Systems Security** и выполните одно из следующих действий:

   - В панели результатов узла перейдите по ссылке **Свойства программы**.
   - В контекстном меню узла выберите пункт **Свойства**.

   Откроется окно **Параметры программы**.

2. На закладке **Безопасность и надежность** в разделе **Параметры применения пароля** установите флажок **Использовать защиту паролем**.

   Поля **Пароль** и **Подтверждение пароля** станут активными.

3. В поле **Пароль** введите пароль, который вы хотите использовать для защиты доступа к функциям Kaspersky Embedded Systems Security.

4. В поле **Подтверждение пароля** введите пароль повторно.

5. Нажмите на кнопку **OK**.

Установленный пароль невозможно восстановить. Утеря пароля ведет к полной потере контроля над программой. Кроме того, невозможно будет удалить программу с защищаемого устройства.

Сбросить пароль можно в любой момент. Для этого снимите флажок **Использовать защиту паролем** и сохраните изменения. Защита паролем будет выключена, и контрольная сумма старого пароля будет удалена. Повторите процесс создания для нового пароля.

Управление правами доступа с помощью Веб-плагина

В этом разделе описана навигация в интерфейсе Веб-плагина и настройка прав доступа для защищаемых устройств сети.

Настройка прав доступа к Kaspersky Embedded Systems Security и службе Kaspersky Security

Чтобы настроить права доступа для пользователя или группы, необходимо указать строку дескриптора безопасности с помощью языка описания дескрипторов безопасности (SDDL). Дополнительная информация о строке дескриптора безопасности приведена на веб-сайте Microsoft.

Чтобы настроить права доступа для пользователя или группы, выполните следующие действия:

1. В главном окне веб-консоли выберите **Устройства** → **Политики и профили**.
2. Выберите политику, которую вы хотите настроить.
3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.
4. Выберите раздел **Дополнительные возможности**.
5. Выполните одно из следующих действий:
   - Нажмите на кнопку **Параметры** в подразделе **Права пользователей на управление программой**, если вы хотите изменить список пользователей, которые имеют доступ к управлению функциями Kaspersky Embedded Systems Security.
   - Нажмите на кнопку **Параметры** в подразделе **Права пользователей на управление службой Kaspersky Security**, если вы хотите изменить список пользователей, которые имеют доступ на управление службой Kaspersky Security.
6. Добавьте пользователя или группу, указав строку дескриптора безопасности в окне **Права пользователей на управление программой** или **Права пользователей на управление службой Kaspersky Security**.
7. Нажмите на кнопку **OK**.

Защита доступа к функциям Kaspersky Embedded Systems Security с помощью пароля

Настройка прав пользователей позволяет ограничивать доступ к управлению программой и регистрируемыми службами. Для дополнительной защиты критических операций можно также установить защиту паролем в параметрах Kaspersky Embedded Systems Security.

Kaspersky Embedded Systems Security запрашивает ввод пароля при попытке доступа к следующим функциям программы:

- подключение к Консоли программы;
- удаление Kaspersky Embedded Systems Security;
- изменение состава компонентов Kaspersky Embedded Systems Security;
- выполнение команд командной строки.

Интерфейс Kaspersky Embedded Systems Security скрывает вводимый пароль на экране. Kaspersky Embedded Systems Security хранит пароль в виде контрольной суммы, рассчитываемой при вводе пароля.

Можно импортировать и экспортировать конфигурацию программ, защищенных паролем. Конфигурационный файл, созданный при экспорте конфигурации защищенной программы, содержит контрольную сумму пароля и значение модификатора, используемого для заполнения строки пароля.

Не изменяйте контрольную сумму и модификатор в конфигурационном файле. Импорт защищенной паролем конфигурации, измененной вручную, может вызвать полную блокировку доступа к программе.

Чтобы защитить доступ к функциям Kaspersky Embedded Systems Security, выполните следующие действия:

1. В главном окне веб-консоли выберите **Устройства** → **Политики и профили**.
2. Выберите политику, которую вы хотите настроить.
3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.
4. Перейдите в раздел **Параметры программы**.
5. В разделе **Безопасность** нажмите на кнопку **Параметры**.
6. В разделе **Параметры применения пароля** установите флажок **Использовать защиту паролем**.
7. В поле **Пароль** введите пароль, который вы хотите использовать для защиты доступа к функциям Kaspersky Embedded Systems Security.
8. Нажмите на кнопку **ОК**.

Настроенные параметры будут сохранены. Kaspersky Embedded Systems Security будет запрашивать указанный пароль для доступа к защищенным функциям.

Установленный пароль невозможно восстановить. Потеря пароля приведет к полной потере контроля над программой. Кроме того, невозможно будет удалить программу с защищаемого устройства.

Сбросить пароль можно в любой момент. Для этого снимите флажок **Использовать защиту паролем** и сохраните изменения. Защита паролем будет выключена, и контрольная сумма старого пароля будет удалена. Повторите процесс создания для нового пароля.

Постоянная защита файлов

Этот раздел содержит информацию о задаче Постоянная защита файлов и инструкции о том, как настроить параметры этой задачи.

О задаче Постоянная защита файлов

В ходе выполнения задачи Постоянная защита файлов Kaspersky Embedded Systems Security проверяет следующие объекты защищаемого устройства при доступе к ним:

- файлы;
- альтернативные потоки данных NTFS;
- основную загрузочную запись и загрузочные секторы локальных жестких дисков и внешних устройств.

При записи или считывании файла любой программой на защищаемом устройстве, Kaspersky Embedded Systems Security перехватывает этот файл, проверяет его на наличие угроз и при обнаружении угрозы выполняет действия, указанные в параметрах задачи или заданные по умолчанию: пытается вылечить файл, перемещает файл на карантин или удаляет его. Перед лечением или удалением Kaspersky Embedded Systems Security сохраняет зашифрованную копию исходного файла в папку резервного хранилища.

Kaspersky Embedded Systems Security также обнаруживает вредоносную активность в процессах подсистемы Windows Subsystem for Linux®. Для таких процессов задача Постоянная защита файлов применяет действие, указанное в текущих параметрах.

Об области защиты и параметрах безопасности задачи

По умолчанию под действие задачи Постоянная защита файлов подпадают все объекты файловой системы устройства. Если по требованиям к безопасности нет необходимости защищать все объекты файловой системы или вы намеренно хотите исключить некоторые объекты из области действия задачи постоянной защиты, вы можете ограничить область защиты.

В Консоли программы область защиты представляет собой дерево или список файловых ресурсов устройства, контролируемых Kaspersky Embedded Systems Security. По умолчанию сетевые файловые ресурсы устройства отображаются в виде списка.

В Плагине управления доступно только представление в виде списка.

Чтобы перейти к отображению сетевых файловых ресурсов в виде дерева в Консоли программы,

в раскрывающемся списке в левом верхнем углу окна **Настройка области защиты** выберите элемент **Показывать в виде дерева**.

Независимо от того, отображаются ли файловые ресурсы защищаемого устройства в виде списка или в виде дерева, значки узлов имеют следующие значения:

☑ – узел включен в область защиты.

☐ – узел исключен из области защиты.

– по крайней мере один из узлов, вложенных в этот узел, исключен из области защиты, или параметры безопасности вложенных узлов отличаются от параметров безопасности родительского узла (только при отображении в виде дерева).

Значок отображается, если выбраны все вложенные узлы, но не выбран родительский узел. В этом случае изменения состава файлов и папок родительского узла не учитываются автоматически при формировании области защиты для выбранного вложенного узла.

С помощью Консоли программы можно также добавлять в область защиты виртуальные диски. Имена виртуальных узлов отображаются синим цветом.

Параметры безопасности

Можно настроить как единые параметры безопасности задачи для всех узлов или элементов, входящих в область защиты, так и различные для всех узлов или элементов в дереве или списке файловых ресурсов устройства.

Параметры безопасности, настроенные для выбранного родительского узла, автоматически применяются для всех вложенных узлов. Параметры безопасности родительского узла не применяются к вложенному узлу, который настраивается отдельно.

Вы можете настроить параметры выбранной области защиты одним из следующих способов:

- выбрать один из трех стандартных уровней безопасности;
- настроить параметры безопасности вручную для выбранных узлов или элементов в дереве или списке файловых ресурсов (уровень безопасности изменится на **Другой**).

Вы можете сохранить набор параметров узла или элемента в шаблон, чтобы потом применять этот шаблон для других узлов или элементов.

О виртуальной области защиты

Kaspersky Embedded Systems Security может проверять не только существующие папки и файлы на жестких и съемных дисках, но и диски, которые динамически создаются на защищаемом устройстве различными программами и службами.

Если все объекты устройства включены в область защиты, эти динамические узлы автоматически войдут в область защиты. Однако если вы хотите задать специальные значения параметров безопасности для динамических узлов или если вы выбрали для защиты отдельные области устройства, то, для того чтобы включить в область защиты виртуальные диски, файлы или папки, вам нужно предварительно создать их в Консоли программы, то есть задать виртуальную область защиты. Созданные диски, файлы и папки существуют только в Консоли программы, но не в структуре файловой системы защищаемого устройства.

Если, формируя область защиты, вы выберете все вложенные папки или файлы, но не выберете родительскую папку, все появившиеся в ней виртуальные папки или файлы не будут автоматически включены в область защиты. Вам нужно создать их виртуальные копии в Консоли программы и добавить их в область защиты.

Стандартные области защиты

В дереве или списке файловых ресурсов отображаются узлы, к которым у вас есть доступ на чтение в соответствии с настроенными параметрами безопасности Microsoft Windows.

В Kaspersky Embedded Systems Security предусмотрены следующие стандартные области защиты:

- **Локальные жесткие диски**. Kaspersky Embedded Systems Security защищает файлы на жестких дисках устройства.
- **Съемные диски**. Kaspersky Embedded Systems Security защищает файлы на внешних устройствах, таких как компакт-диски или съемные диски. Вы можете включать в область защиты или исключать из нее все съемные диски, а также отдельные диски, папки или файлы.
- **Сетевое окружение**. Kaspersky Embedded Systems Security защищает файлы, которые записываются в сетевые папки или считываются из них программами, выполняемыми на устройстве. Kaspersky Embedded Systems Security не защищает файлы, когда к ним обращаются программы с других защищаемых устройств.
- **Виртуальные диски**. Можно включать в область защиты виртуальные папки и файлы, а также диски, временно подключенные к устройству, например, общие диски кластера.

Стандартные области защиты по умолчанию отображаются и доступны для изменения в списке областей; можно также добавлять стандартные области защиты в список при его формировании в параметрах области защиты.

По умолчанию в область защиты включены все стандартные области, кроме виртуальных дисков.

Виртуальные диски, созданные с помощью команды SUBST, не отображаются в дереве файловых ресурсов защищаемого устройства в Консоли программы. Чтобы включить в область защиты объекты на виртуальном диске, включите в область защиты папку на устройстве, связанную с этим виртуальным диском.

Подключенные сетевые диски также не отображаются в списке файловых ресурсов защищаемого устройства. Чтобы включить в область защиты объекты на сетевом диске, укажите путь к папке, соответствующей этому сетевому диску, в формате UNC (Universal Naming Convention).

Стандартные уровни безопасности

Для выбранных в дереве или списке файловых ресурсов защищаемого устройства узлов можно задать один из следующих стандартных уровней безопасности: **Максимальное быстродействие**, **Рекомендуемый** или **Максимальная защита**. Каждый из этих уровней имеет свой стандартный набор значений параметров безопасности (см. таблицу ниже).

Максимальное быстродействие

Уровень безопасности **Максимальное быстродействие** рекомендуется применять, если в вашей сети, наряду с использованием Kaspersky Embedded Systems Security на защищаемых устройствах, применяются дополнительные меры безопасности, например, сетевые экраны и политики безопасности.

Рекомендуемый

Уровень безопасности **Рекомендуемый** обеспечивает оптимальное сочетание качества защиты и влияния на производительность устройств. Этот уровень рекомендован специалистами "Лаборатории Касперского" как достаточный для защиты устройств в большинстве сетей организаций. Уровень безопасности **Рекомендуемый** установлен по умолчанию.

Максимальная защита

Уровень безопасности **Максимальная защита** рекомендуется применять, если предъявляются повышенные требования к безопасности устройств в сети организации.

Стандартные уровни безопасности и соответствующие им значения параметров

Параметры	Уровень безопасности		
	Максимальное быстродействие	Рекомендуемый	Максимальная защита
Защита объектов	По расширению	По формату	По формату
Проверка только новых и измененных файлов	Включена	Включена	Выключено
Действия над зараженными и другими обнаруженными объектами	Блокировать доступ и лечить. Удалить, если не удалось вылечить.	Блокировать доступ и лечить. Удалить, если не удалось вылечить.	Блокировать доступ и лечить. Удалить, если не удалось вылечить.
Действия над возможно зараженными объектами	Блокировать доступ и поместить на карантин.	Блокировать доступ и поместить на карантин.	Блокировать доступ и поместить на карантин.
Исключать файлы	Нет	Нет	Нет
Не обнаруживать	Нет	Нет	Нет
Останавливать проверку, если она длится более (сек.)	60 сек.	60 сек.	60 сек.
Не проверять составные объекты размером более (МБ)	8 МБ	8 МБ	Не установлен
Альтернативные потоки NTFS	Да	Да	Да
Загрузочные секторы дисков и MBR	Да	Да	Да
Защита составных объектов	• Упакованные объекты* * Только новые и измененные	• SFX-архивы* • Упакованные объекты* • Вложенные OLE-объекты* * Только новые и измененные	• SFX-архивы* • Упакованные объекты* • Вложенные OLE-объекты* * Все объекты
Полностью удалять составной файл при обнаружении вложенного объекта, если	Нет	Нет	Да

составной файл не может быть изменен программой			

Параметры **Защита объектов**, **Использовать технологию iChecker**, **Использовать технологию iSwift** и **Использовать эвристический анализатор** не входят в набор параметров стандартных уровней безопасности. Если, выбрав один из стандартных уровней безопасности, вы измените параметры безопасности **Защита объектов**, **Использовать технологию iChecker**, **Использовать технологию iSwift** или **Использовать эвристический анализатор**, выбранный вами стандартный уровень безопасности не изменится.

Расширения файлов, проверяемые по умолчанию в задаче Постоянная защита файлов

По умолчанию Kaspersky Embedded Systems Security проверяет файлы, имеющие следующие расширения:

- *386;*
- *acm;*
- *ade, adp;*
- *asp;*
- *asx;*
- *ax;*
- *bas;*
- *bat;*
- *bin;*
- *chm;*
- *cla, clas*;*
- *cmd;*
- *com;*
- *cpl;*
- *crt;*
- *dll;*
- *dpl;*
- *drv;*

- *dvb;*
- *dwg;*
- *efi;*
- *emf;*
- *eml;*
- *exe;*
- *fon;*
- *fpm;*
- *hlp;*
- *hta;*
- *htm, html*;*
- *htt;*
- *ico;*
- *inf;*
- *ini;*
- *ins;*
- *isp;*
- *jpg, jpe;*
- *js, jse;*
- *lnk;*
- *mbx;*
- *msc;*
- *msg;*
- *msi;*
- *msp;*
- *mst;*
- *nws;*
- *ocx;*

- *oft;*
- *otm;*
- *pcd;*
- *pdf;*
- *php;*
- *pht;*
- *phtm*;*
- *pif;*
- *plg;*
- *png;*
- *pot;*
- *prf;*
- *prg;*
- *reg;*
- *rsc;*
- *rtf;*
- *scf;*
- *scr;*
- *sct;*
- *shb;*
- *shs;*
- *sht;*
- *shtm*;*
- *swf;*
- *sys;*
- *the;*
- *them*;*
- *tsp;*

- *url;*
- *vb;*
- *vbe;*
- *vbs;*
- *vxd;*
- *wma;*
- *wmf;*
- *wmv;*
- *wsc;*
- *wsf;*
- *wsh;*
- *do?;*
- *md?;*
- *mp?;*
- *ov?;*
- *pp?;*
- *vs?;*
- *xl?*

Параметры задачи Постоянная защита файлов по умолчанию

По умолчанию в задаче Постоянная защита файлов используются параметры, описанные в таблице ниже. Вы можете изменять значения этих параметров.

Параметры задачи Постоянная защита файлов по умолчанию

Параметр	Значение по умолчанию	Описание
Область защиты	Защищаемое устройство целиком, исключая виртуальные диски.	Вы можете изменить область защиты.
Параметры безопасности	Единые для всей области защиты; соответствует уровню безопасности **Рекомендуемый**.	Для узлов, выбранных в дереве или списке файловых ресурсов защищаемого устройства, можно выполнить следующие действия:

		• выбрать другой стандартный уровень безопасности; • вручную изменить параметры безопасности. Вы можете сохранить набор параметров безопасности выбранного узла как шаблон, чтобы потом применить его для другого узла.
Режим защиты объектов	**При открытии и изменении**	Вы можете выбрать режим защиты – указать, при каком типе доступа к объектам Kaspersky Embedded Systems Security проверяет их.
Эвристический анализатор	Применяется уровень безопасности **Средний**.	Вы можете включать и выключать эвристический анализатор, а также регулировать уровень анализа.
Применять доверенную зону	Применяется.	Единый список исключений, который можно применять в выбранных задачах.
Использовать KSN для защиты	Применяется.	Вы можете увеличить эффективность защиты устройства с помощью облачных служб Kaspersky Security Network (доступных, если принято Положение о KSN).
Расписание запуска задачи	При запуске программы.	Вы можете настроить запуск задачи по расписанию.
Блокировать доступ к сетевым файловым ресурсам для узлов, с которых ведется вредоносная активность	Не применяется.	Вы можете добавлять узлы, со стороны которых выявлена вредоносная активность, в список заблокированных узлов.
Запустить сканирование важных областей при обнаружении активного заражения	Применяется.	При обнаружении активного заражения Kaspersky Embedded Systems Security создает и запускает временную задачу Проверка важных областей.

Управление задачей Постоянная защита файлов с помощью Плагина управления

В этом разделе описана навигация в интерфейсе Плагина управления и настройка параметров задачи для защищаемых устройств в сети.

Навигация

В этом разделе описан переход к требуемым параметрам задачи с помощью интерфейса.

Переход к параметрам политики для задачи Постоянная защита файлов

Чтобы перейти к параметрам задачи Постоянная защита файлов в политике Kaspersky Security Center, выполните следующие действия:

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой вы хотите настроить задачу.
3. Выберите закладку **Политики**.
4. Откройте окно свойств политики двойным щелчком мыши на имени политики, которую вы хотите настроить.
5. В открывшемся окне **Свойства: <Имя политики>** перейдите в раздел **Постоянная защита компьютера**.
6. Нажмите на кнопку **Настройка** в подразделе **Постоянная защита файлов**.

   Откроется окно **Постоянная защита файлов**.

Если защищаемое устройство работает под управлением активной политики Kaspersky Security Center и в этой политике запрещено изменение параметров программы, эти параметры недоступны для изменения в Консоли программы.

Переход к параметрам задачи Постоянная защита файлов

Чтобы перейти к окну параметров задачи Постоянная защита файлов для отдельного устройства, выполните следующие действия:

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой вы хотите настроить задачу.
3. Выберите закладку **Устройства**.
4. Откройте окно **Свойства: <Имя защищаемого устройства>** одним из следующих способов:

   - двойным щелчком мыши на имени защищаемого устройства;
   - выбрав пункт **Свойства** в контекстном меню защищаемого устройства.

   Откроется окно **Свойства: <Имя защищаемого устройства>**.
5. В блоке **Задачи** выберите задачу **Постоянная защита файлов**.
6. Нажмите на кнопку **Свойства**.

   Откроется окно **Свойства: Постоянная защита файлов**.

Настройка задачи Постоянная защита файлов

Чтобы настроить параметры задачи Постоянная защита файлов, выполните следующие действия:

1. Откройте окно **Постоянная защита файлов**.
2. Настройте следующие параметры задачи:
   - На закладке **Общие**:
     - **Режим защиты объектов**
     - **Эвристический анализатор**
     - **Интеграция с другими компонентами**
   - На закладке **Управление задачей**:
     - Запуск задачи по расписанию.
3. Выберите закладку **Область защиты** и выполните следующие действия:
   - Нажмите на кнопку **Добавить** или **Изменить**, чтобы изменить область защиты.
     - В открывшемся окне выберите, что требуется включить в область защиты задачи:
       - **Предопределенная область**
       - **Диск, папка или сетевой объект**
       - **Файл**
     - Выберите один из стандартных уровней безопасности или настройте параметры защиты вручную.
4. Нажмите на кнопку **ОК** в окне **Постоянная защита файлов**.

Kaspersky Embedded Systems Security немедленно применит новые значения параметров в выполняющейся задаче. Дата и время изменения параметров, а также значения параметров задачи до и после изменения будут сохранены в журнале системного аудита.

Выбор режима защиты

В задаче Постоянная защита файлов вы можете выбрать режим защиты объектов. В разделе **Режим защиты объектов** можно указать, при каком типе доступа к объектам Kaspersky Embedded Systems Security проверяет эти объекты.

Значение параметра **Режим защиты объектов** применяется для всей области защиты, указанной в задаче. Вы не можете установить различные значения параметра для отдельных узлов области защиты.

Чтобы выбрать режим защиты, выполните следующие действия:

1. Откройте окно **Постоянная защита файлов**.
2. В открывшемся окне на закладке **Общие** выберите режим защиты, который вы хотите установить:
   - **Интеллектуальный режим**
   - **При открытии и изменении**
   - **При открытии**
   - **При выполнении**
3. Нажмите на кнопку **OK**.

Выбранный режим защиты объектов будет установлен.

Настройка эвристического анализатора и интеграции с другими компонентами программы

Для запуска задачи Использование KSN необходимо принять Положение о Kaspersky Security Network.

Чтобы настроить эвристический анализатор и интеграцию с другими компонентами, выполните следующие действия:

1. Откройте окно **Постоянная защита файлов**.
2. На закладке **Общие** снимите или установите флажок **Использовать эвристический анализатор**.
3. Если требуется, отрегулируйте уровень анализа с помощью ползунка.
4. В разделе **Интеграция с другими компонентами** настройте следующие параметры:
   - Установите или снимите флажок **Применять доверенную зону**.
   - Установите или снимите флажок **Использовать KSN для защиты**.

     Флажок **Разрешить отправку данных о проверяемых файлах** должен быть установлен в параметрах задачи Использование KSN.

   - Установите или снимите флажок **Блокировать доступ к сетевым файловым ресурсам для узлов, с которых ведется вредоносная активность**.
   - Снимите или установите флажок **Запустить сканирование важных областей при обнаружении активного заражения**.
5. Нажмите на кнопку **OK**.

Настроенные параметры задачи будут применены немедленно в выполняющейся задаче. Если задача не выполняется, измененные параметры будут применены при ее последующем запуске.

Настройка расписания запуска задач

В Консоли программы вы можете настроить расписание запуска локальных системных и пользовательских задач. Расписание запуска групповых задач настраивать нельзя.

Чтобы настроить расписание запуска групповой задачи, выполните следующие действия:

1. В дереве Консоли администрирования Kaspersky Security Center разверните узел **Управляемые устройства**.
2. Выберите группу, к которой принадлежит защищаемое устройство.
3. В панели результатов выберите закладку **Задачи**.
4. Откройте окно **Свойства: <Название задачи>** одним из следующих способов:
   - двойным щелчком мыши по имени задачи;
   - выбрав пункт Свойства в контекстном меню задачи.
5. Выберите раздел **Расписание**.
6. В блоке **Параметры расписания** установите флажок **Запускать задачу по расписанию**.

   Поля с параметрами расписания задачи проверки по требованию и задачи обновления недоступны, если запуск этих задач по расписанию запрещен политикой Kaspersky Security Center.

7. Настройте параметры расписания в соответствии с вашими требованиями. Для этого выполните следующие действия:

   a. в списке **Частота запуска** выберите одно из следующих значений:

   - **Ежечасно**, если вы хотите, чтобы задача запускалась периодически через заданное количество часов, и укажите количество часов в поле **Раз в <количество> часов**.
   - **Ежесуточно**, если вы хотите, чтобы задача запускалась периодически через заданное количество дней, и укажите количество дней в поле **Раз в <количество> дней**.
   - **Еженедельно**, если вы хотите, чтобы задача запускалась периодически через заданное количество недель, и укажите количество недель в поле **Раз в <количество> недель**. Укажите, по каким дням недели будет запускаться задача (по умолчанию задача запускается по понедельникам).
   - **При запуске программы**, если вы хотите, чтобы задача запускалась при каждом запуске Kaspersky Embedded Systems Security.
   - **После обновления баз программы**, если вы хотите, чтобы задача запускалась после каждого обновления баз программы.

   b. В поле **Время запуска** укажите время первого запуска задачи.

   c. В поле **Начать с** укажите дату начала действия расписания.

После того как вы укажете частоту и время первого запуска задачи и дату начала действия расписания, в верхней части окна в поле **Следующий запуск** отобразится расчетное время очередного запуска задачи. Расчетное время следующего запуска задачи будет обновляться каждый раз, когда вы открываете окно **Параметры задачи** на закладке **Расписание**.

Значение **Запрещен политикой** отображается в поле **Следующий запуск**, если параметрами действующей политики Kaspersky Security Center запрещен запуск системных задач по расписанию.

8. На закладке **Дополнительно** настройте следующие параметры расписания в соответствии с вашими требованиями.
   - В блоке **Параметры остановки задачи**:
     a. Установите флажок **Длительность** и в полях справа укажите максимальную длительность выполнения задачи (количество часов и минут).
     b. Установите флажок **Приостановить с** и в полях справа укажите начальное и конечное значение временного промежутка в пределах суток, в течение которого выполнение задачи будет приостановлено.
   - В блоке **Дополнительные параметры**:
     a. Установите флажок **Отменить расписание с** и укажите дату, начиная с которой расписание перестанет действовать.
     b. Установите флажок **Запускать пропущенные задачи**, чтобы включить запуск пропущенных задач.
     c. Установите флажок **Распределять время запуска задач в интервале** и укажите значение параметра в минутах.
9. Нажмите на кнопку **ОК**.
10. Нажмите на кнопку **Применить**, чтобы сохранить параметры запуска задачи.

Если вы хотите настроить параметры программы для отдельной задачи с помощью Kaspersky Security Center, выполните действия, описанные в разделе "Настройка локальных задач в окне Параметры программы в Kaspersky Security Center".

Создание и настройка области защиты задачи

Чтобы создать и настроить область защиты задачи в Kaspersky Security Center, выполните следующие действия:

1. Откройте окно **Постоянная защита файлов**.
2. Выберите закладку **Область защиты**.

3. Все элементы, на которые распространяется область защиты задачи, перечислены в таблице **Область защиты**.

4. Нажмите на кнопку **Добавить**, чтобы добавить в список новый элемент.

   Откроется окно **Добавление в область защиты**.

5. Выберите тип объектов для добавления в область защиты:

   - **Предопределенная область**, чтобы включить в область защиты одну из стандартных областей на устройстве. Затем в раскрывающемся списке выберите требуемую область защиты.
   - **Диск, папка или сетевой объект**, чтобы включить в область защиты отдельный диск, папку или сетевой объект. Затем выберите нужную область защиты по кнопке **Обзор**.
   - **Файл**, чтобы включить в область защиты отдельный файл. Затем выберите нужную область защиты по кнопке **Обзор**.

   Нельзя добавить объект в область защиты, если он уже добавлен в качестве исключения из области защиты.

6. Чтобы исключить отдельные элементы из области защиты, снимите флажки рядом с именами этих элементов или выполните следующие действия:

   a. Откройте контекстное меню области защиты по правой клавише мыши.

   b. В контекстном меню выберите пункт **Добавить исключение**.

   c. В окне **Добавление исключения** выберите тип объектов, который вы хотите добавить в качестве исключения из области защиты, по аналогии с добавлением объекта в область защиты.

7. Чтобы изменить область защиты или исключение, в контекстном меню требуемой области защиты выберите пункт **Изменить область**.

8. Чтобы скрыть добавленную ранее область защиты или исключение в списке сетевых файловых ресурсов, в контекстном меню требуемой области защиты выберите пункт **Удалить область**.

   Область защиты будет удалена из области действия задачи Постоянная защита файлов при ее удалении из списка сетевых файловых ресурсов.

9. Нажмите на кнопку **ОК**.

Окно Параметры области защиты закроется. Настроенные параметры будут сохранены.

Задачу **Постоянная защита файлов** можно запустить, если по крайней мере один узел файловых ресурсов устройства включен в область защиты.

Выбор стандартных уровней безопасности в задачах проверки по требованию

Для выбранного в дереве файловых ресурсов узла можно задать один из следующих стандартных уровней безопасности: **Максимальное быстродействие**, **Рекомендуемый** или **Максимальная защита**.

Чтобы выбрать один из стандартных уровней безопасности, выполните следующие действия:

1. Откройте окно **Свойства: Постоянная защита файлов**.
2. Выберите закладку **Область защиты**.
3. В списке защищаемых устройств выберите элемент, включенный в область защиты, чтобы задать для него стандартный уровень безопасности.
4. Нажмите на кнопку **Настроить**.

   Откроется окно **Настройка параметров постоянной защиты файлов**.
5. На закладке **Уровень безопасности** выберите требуемый уровень безопасности.

   В окне отобразится список значений параметров безопасности, которые соответствуют выбранному вами уровню безопасности.
6. Нажмите на кнопку **OK**.
7. Нажмите на кнопку **OK** в окне **Свойства: Постоянная защита файлов**.

   Настроенные параметры задачи будут сохранены и применены немедленно в выполняющейся задаче. Если задача не выполняется, измененные параметры будут применены при ее последующем запуске.

Настройка параметров безопасности вручную

По умолчанию в задаче Постоянная защита файлов применяются единые параметры безопасности для всей области защиты. Эти параметры соответствуют стандартному уровню безопасности **Рекомендуемый**.

Можно изменять значения параметров безопасности, заданные по умолчанию, настроив их как едиными для всей области защиты, так и различными для отдельных элементов в дереве или списке файловых ресурсов устройства.

Чтобы вручную настроить параметры безопасности выбранного узла, выполните следующие действия:

1. Откройте окно **Постоянная защита файлов**.
2. На закладке **Область защиты** выберите узел, параметры безопасности которого вы хотите настроить, и нажмите на кнопку **Настроить**.

   Откроется окно **Настройка параметров постоянной защиты файлов**.
3. На закладке **Уровень безопасности** нажмите на кнопку **Настройка**.
4. Вы можете настроить пользовательские параметры безопасности для выбранного узла в соответствии с вашими требованиями:

   - Общие параметры
   - Действия
   - Производительность

5. Нажмите на кнопку **OK** в окне **Постоянная защита файлов**.

Новые параметры области защиты будут сохранены.

Настройка общих параметров задачи

Чтобы настроить общие параметры безопасности задачи Постоянная защита файлов, выполните следующие действия.

1. Откройте окно **Настройка параметров постоянной защиты файлов**.
2. Выберите закладку **Общие**.
3. В блоке **Защита объектов** укажите типы объектов, которые вы хотите включить в область защиты:
   - Все объекты
   - **Объекты, проверяемые по формату**
   - **Объекты, проверяемые по списку расширений, указанному в антивирусных базах**
   - **Объекты, проверяемые по указанному списку расширений**
   - **Загрузочные секторы дисков и MBR**
   - **Альтернативные потоки NTFS**
4. В блоке параметров **Оптимизация** установите или снимите флажок **Проверка только новых и измененных файлов**.

   Для переключения между доступными вариантами при снятом флажке перейдите по ссылке Все / Только новые для каждого типа составных объектов.

5. В блоке **Защита составных объектов** укажите составные объекты, которые вы хотите включить в область защиты:
   - Все / **Только новые архивы**
   - Все / **Только новые SFX-архивы**
   - Все / **Только новые почтовые базы**
   - Все / **Только новые упакованные объекты**
   - Все / **Только новые файлы почтовых форматов**
   - Все / **Только новые вложенные OLE-объекты**
6. Нажмите на кнопку **Сохранить**.

Новая конфигурация задачи будет сохранена.

Настройка действий

Чтобы настроить действия, которые задача Постоянная защита файлов выполняет над зараженными и другими обнаруженными объектами, выполните следующие действия:

1. Откройте окно **Настройка параметров постоянной защиты файлов**.
2. Выберите закладку **Действия**.
3. Выберите действие над зараженными и другими обнаруживаемыми объектами:
   - **Только сообщать**
   - **Блокировать доступ**
   - **Выполнять дополнительное действие**

     Выберите действие из раскрывающегося списка:
     - **Лечить**
     - **Лечить. Удалять, если лечение невозможно**
     - **Удалять**
     - **Рекомендуемое**
4. Выберите действие над возможно зараженными объектами:
   - **Только сообщать**
   - **Блокировать доступ**
   - **Выполнять дополнительное действие**

     Выберите действие из раскрывающегося списка:
     - **Помещать на карантин**
     - **Удалять**
     - **Рекомендуемое**
5. Настройте действия над объектами в зависимости от типа обнаруженного объекта:
   a. Снимите или установите флажок **Выполнять действия в зависимости от типа обнаруженного объекта**.
   b. Нажмите на кнопку **Настройка**.
   c. В открывшемся окне выберите первичное действие и (на случай неудачного выполнения первичного действия) вторичное действие для каждого типа обнаруженного объекта.
   d. Нажмите на кнопку **OK**.

6. Выберите действие над неизменяемыми составными файлами: снимите или установите флажок **Полностью удалять составной файл при обнаружении вложенного объекта, если составной файл не может быть изменен программой**.

7. Нажмите на кнопку **Сохранить**.

Новая конфигурация задачи будет сохранена.

Настройка производительности

Чтобы настроить параметры производительности задачи Постоянная защита файлов, выполните следующие действия:

1. Откройте окно **Настройка параметров постоянной защиты файлов**.

2. Выберите закладку **Производительность**.

3. В блоке **Исключения**:

   - Снимите или установите флажок **Исключать файлы**.
   - Снимите или установите флажок **Не обнаруживать**.
   - Нажмите на кнопку **Изменить** для каждого параметра, чтобы добавить исключения.

4. В блоке **Дополнительные параметры**:

   - **Останавливать проверку, если она длится более (сек.)**
   - **Не проверять составные объекты размером более (МБ)**
   - **Использовать технологию iSwift**
   - **Использовать технологию iChecker**

Управление задачей Постоянная защита файлов с помощью Консоли программы

В этом разделе описана навигация в интерфейсе Консоли программы и настройка параметров задачи на защищаемом устройстве.

Навигация

В этом разделе описан переход к требуемым параметрам задачи с помощью интерфейса.

Переход к параметрам задачи Постоянная защита файлов

Чтобы перейти к окну общих параметров задачи, выполните следующие действия:

1. В дереве Консоли программы разверните узел **Постоянная защита компьютера**.
2. Выберите вложенный узел **Постоянная защита файлов**.
3. В панели результатов перейдите по ссылке **Свойства**.
   Откроется окно **Параметры задачи**.

Переход к параметрам области действия задачи Постоянная защита файлов

Чтобы перейти к окну параметров области защиты для задачи Постоянная защита файлов, выполните следующие действия.

1. В дереве Консоли программы разверните узел **Постоянная защита компьютера**.
2. Выберите вложенный узел **Постоянная защита файлов**.
3. В панели результатов перейдите по ссылке **Настроить область защиты**.
   Откроется окно **Настройка области защиты**.

Настройка задачи Постоянная защита файлов

Чтобы настроить параметры задачи Постоянная защита файлов, выполните следующие действия:

1. Откройте окно **Параметры задачи**.
2. На закладке **Общие** настройте следующие параметры задачи:
   - Режим защиты объектов
   - **Эвристический анализатор**
   - **Интеграция с другими компонентами**
3. На закладках **Расписание** и **Дополнительно** настройте расписание задачи.
4. В окне **Параметры задачи** нажмите на кнопку **OK**.
   Изменения параметров задачи будут сохранены.
5. В панели результатов узла **Постоянная защита файлов** перейдите по ссылке **Настроить область защиты**.
6. Выполните следующие действия:
   - В дереве или списке файловых ресурсов устройства выберите узлы или элементы, которые вы хотите включить в область защиты задачи.

- Выберите один из стандартных уровней безопасности или настройте параметры защиты объекта вручную.

7. В окне **Настройка области защиты** нажмите на кнопку **Сохранить**.

Kaspersky Embedded Systems Security немедленно применит новые значения параметров в выполняющейся задаче. Дата и время изменения параметров, а также значения параметров задачи до и после изменения будут сохранены в журнале системного аудита.

Выбор режима защиты объектов

В задаче Постоянная защита файлов вы можете выбрать режим защиты объектов. В разделе **Режим защиты объектов** можно указать, при каком типе доступа к объектам Kaspersky Embedded Systems Security проверяет эти объекты.

Значение параметра **Режим защиты объектов** применяется для всей области защиты, указанной в задаче. Вы не можете установить различные значения параметра для отдельных узлов области защиты.

Чтобы выбрать режим защиты, выполните следующие действия:

1. Откройте окно **Параметры задачи**.
2. В открывшемся окне на закладке **Общие** выберите режим защиты, который вы хотите установить:
   - **Интеллектуальный режим**
   - **При открытии и изменении**
   - **При открытии**
   - **При выполнении**
3. Нажмите на кнопку **ОК**.

Выбранный режим защиты объектов будет установлен.

Настройка эвристического анализатора и интеграции с другими компонентами программы

Для запуска задачи Использование KSN необходимо принять Положение о Kaspersky Security Network.

Чтобы настроить эвристический анализатор и интеграцию с другими компонентами, выполните следующие действия:

1. Откройте окно **Параметры задачи**.
2. На закладке **Общие** снимите или установите флажок **Использовать эвристический анализатор**.
3. Если требуется, отрегулируйте уровень анализа с помощью ползунка.

4. В разделе **Интеграция с другими компонентами** настройте следующие параметры:

   - Установите или снимите флажок **Применять доверенную зону**.

     По ссылке **Доверенная зона** перейдите к параметрам доверенной зоны.

   - Установите или снимите флажок **Использовать KSN для защиты**.

     > Флажок **Разрешить отправку данных о проверяемых файлах** должен быть установлен в параметрах задачи Использование KSN.

   - Установите или снимите флажок **Блокировать доступ к сетевым файловым ресурсам для узлов, с которых ведется вредоносная активность**.

   - Снимите или установите флажок **Запустить сканирование важных областей при обнаружении активного заражения**.

5. Нажмите на кнопку **OK**.

Настроенные параметры задачи будут применены.

Настройка расписания запуска задач

В Консоли программы вы можете настроить расписание запуска локальных системных и пользовательских задач. Вы не можете настраивать расписание запуска групповых задач.

Чтобы настроить расписание запуска задачи, выполните следующие действия:

1. Откройте контекстное меню задачи, для которой вы хотите настроить расписание запуска.
2. Выберите пункт **Свойства**.

   Откроется окно **Параметры задачи**.
3. В открывшемся окне на закладке **Расписание** установите флажок **Запускать задачу по расписанию**.
4. Настройте параметры расписания в соответствии с вашими требованиями. Для этого выполните следующие действия:

   a. В раскрывающемся списке **Частота запуска** выберите одно из следующих значений:

   - **Ежечасно**, если вы хотите, чтобы задача запускалась периодически через заданное количество часов, и укажите количество часов в поле **Раз в <количество> ч**.
   - **Ежесуточно**, если вы хотите, чтобы задача запускалась периодически через заданное количество дней, и укажите количество дней в поле **Раз в <количество> сут**.
   - **Еженедельно**, если вы хотите, чтобы задача запускалась периодически через заданное количество недель, и укажите количество недель в поле **Раз в <количество> нед. по**. Укажите, по каким дням недели будет запускаться задача (по умолчанию задача запускается по понедельникам).
   - **При запуске программы**, если вы хотите, чтобы задача запускалась при каждом запуске Kaspersky Embedded Systems Security.

- **После обновления баз программы**, если вы хотите, чтобы задача запускалась после каждого обновления баз программы.

b. В поле **Время запуска** укажите время первого запуска задачи.

c. В поле **Начать с** укажите дату начала действия расписания.

После того как вы укажете частоту и время первого запуска задачи и дату начала действия расписания, в верхней части окна в поле **Следующий запуск** отобразится расчетное время очередного запуска задачи. Расчетное время следующего запуска задачи будет обновляться каждый раз, когда вы открываете окно **Параметры задачи** на закладке **Расписание**.

Значение **Запрещен политикой** отображается в поле **Следующий запуск**, если параметрами политики Kaspersky Security Center запрещен запуск системных задач по расписанию.

5. На закладке **Дополнительно** настройте следующие параметры расписания в соответствии с вашими требованиями.

- В блоке **Параметры остановки задачи**:

a. Установите флажок **Длительность** и в полях справа укажите максимальную длительность выполнения задачи (количество часов и минут).

b. Установите флажок **Приостановить с** и в полях справа укажите начальное и конечное значение временного промежутка в пределах суток, в течение которого выполнение задачи будет приостановлено.

- В блоке **Дополнительные параметры**:

a. Установите флажок **Отменить расписание с** и укажите дату, начиная с которой расписание перестанет действовать.

b. Установите флажок **Запускать пропущенные задачи**, чтобы включить запуск пропущенных задач.

c. Установите флажок **Распределить время запуска в интервале** и укажите значение параметра в минутах.

6. Нажмите на кнопку **ОК**.

Настроенные параметры расписания запуска выбранной задачи будут сохранены.

Формирование области защиты

Этот раздел содержит информацию о формировании и использовании области защиты в задаче Постоянная защита файлов и дальнейшей работе с ней.

Настройка отображения сетевых файловых ресурсов

Чтобы выбрать отображение сетевых файловых ресурсов при настройке параметров области защиты, выполните следующие действия:

1. Откройте окно **Настройка области защиты**.
2. В раскрывающемся списке в левом верхнем углу окна выберите один из следующих вариантов:
   - Выберите **Показывать в виде дерева**, чтобы сетевые файловые ресурсы отображались в виде дерева.
   - Выберите **Показывать в виде списка**, чтобы сетевые файловые ресурсы отображались в виде списка.

   По умолчанию сетевые файловые ресурсы защищаемого устройства отображаются в виде списка.
3. Нажмите на кнопку **Сохранить**.

Формирование области защиты

Процедура формирования области действия задачи Постоянная защита файлов зависит от выбранного отображения сетевых файловых ресурсов. Сетевые файловые ресурсы могут отображаться в виде дерева или в виде списка (по умолчанию).

Чтобы применить к задаче новые параметры области защиты, нужно перезапустить задачу Постоянная защита файлов.

Чтобы сформировать область защиты с помощью дерева сетевых файловых ресурсов, выполните следующие действия:

1. Откройте окно **Настройка области защиты**.
2. В левой части окна разверните дерево сетевых файловых ресурсов, чтобы отобразить все узлы.
3. Выполните следующие действия:
   - Чтобы исключить отдельные узлы из области защиты, снимите флажки рядом с именами этих узлов.
   - Чтобы включить отдельные узлы в область защиты, снимите флажок **Мой компьютер** и выполните следующие действия:
     - Если вы хотите включить в область защиты все диски одного типа, установите флажок рядом с названием нужного типа дисков. Например, чтобы включить все съемные диски устройства, установите флажок **Съемные диски**.
     - Если вы хотите включить в область защиты отдельный диск определенного типа, разверните узел, который содержит список дисков этого типа, и установите флажок рядом с именем нужного диска. Например, чтобы выбрать съемный диск F:, разверните узел **Съемные диски** и установите флажок для диска **F:**.
     - Если вы хотите включить в область защиты только отдельную папку или отдельный файл на диске, установите флажок рядом с именем этой папки или этого файла.
4. Нажмите на кнопку **Сохранить**.

Окно **Настройка области защиты** закроется. Настроенные параметры будут сохранены.

Чтобы сформировать область защиты с помощью списка сетевых файловых ресурсов, выполните следующие действия:

1. Откройте окно **Настройка области защиты**.
2. Чтобы включить отдельные узлы в область защиты, снимите флажок **Мой компьютер** и выполните следующие действия:
   a. Откройте контекстное меню области защиты по правой клавише мыши.
   b. В контекстном меню выберите пункт **Добавить область защиты**.
   c. В окне **Добавление области защиты** выберите тип объектов, который вы хотите включить в область защиты:
      - **Предопределенная область**, чтобы включить в область защиты одну из стандартных областей на устройстве. Затем в раскрывающемся списке выберите требуемую область защиты.
      - **Диск, папка или сетевой объект**, чтобы включить в область защиты отдельный диск, папку или сетевой объект. Затем выберите нужную область, нажав на кнопку **Обзор**.
      - **Файл**, чтобы включить в область защиты отдельный файл. Затем выберите нужную область, нажав на кнопку **Обзор**.

   Нельзя добавить объект в область защиты, если он уже добавлен в качестве исключения из области защиты.
3. Чтобы исключить отдельные узлы из области защиты, снимите флажки рядом с именами этих узлов или выполните следующие действия:
   a. Откройте контекстное меню области защиты по правой клавише мыши.
   b. В контекстном меню выберите пункт **Добавить исключение**.
   c. В окне **Добавление исключения** выберите тип объектов, который вы хотите добавить в качестве исключения из области защиты, по аналогии с добавлением объекта в область защиты.
4. Чтобы изменить область защиты или исключение, в контекстном меню требуемой области защиты выберите пункт **Изменить область**.
5. Чтобы скрыть добавленную ранее область защиты или исключения в списке сетевых файловых ресурсов, в контекстном меню требуемой области выберите пункт **Удалить из списка**.

   Область защиты будет удалена из области действия задачи Постоянная защита файлов при ее удалении из списка сетевых файловых ресурсов.
6. Нажмите на кнопку **Сохранить**.

Окно **Настройка области защиты** закроется. Настроенные параметры будут сохранены.

Задачу Постоянная защита файлов можно запустить, если по крайней мере один узел файловых ресурсов устройства включен в область защиты.

Если указана сложная область защиты, например, заданы разные значения параметров безопасности для отдельных узлов в дереве файловых ресурсов устройства, это может привести к замедлению проверки объектов при доступе к ним.

Включение сетевых объектов в область защиты

Вы можете включать в область защиты сетевые диски, папки и файлы, указывая сетевые пути к ним в формате UNC (Universal Naming Convention).

Вы можете проверять сетевые папки при работе под системной учетной записью.

Чтобы включить в область защиты сетевой объект, выполните следующие действия:

1. Откройте окно **Настройка области защиты**.
2. В раскрывающемся списке в левом верхнем углу окна выберите пункт **Показывать в виде дерева**.
3. В контекстном меню узла **Сетевое окружение** выполните следующие действия:
   - Выберите пункт **Добавить сетевую папку**, чтобы добавить сетевую папку в область защиты.
   - Выберите пункт **Добавить сетевой файл**, чтобы добавить сетевой файл в область защиты.
4. Введите путь к сетевой папке или файлу в формате UNC (Universal Naming Convention).
5. Нажмите на клавишу **ENTER**.
6. Установите флажок рядом с именем добавленного сетевого объекта, чтобы включить его в область защиты.
7. Если требуется, измените параметры безопасности для добавленного сетевого объекта.
8. Нажмите на кнопку **Сохранить**.

Настроенные изменения параметров задачи будут сохранены.

Формирование виртуальной области защиты

Вы можете включить в область защиты / проверки отдельные виртуальные диски, папки или файлы, только если область защиты / проверки отображается в виде дерева файловых ресурсов.

Чтобы добавить виртуальный диск в область защиты, выполните следующие действия:

1. Откройте окно **Настройка области защиты**.
2. В раскрывающемся списке в левом верхнем углу окна выберите пункт **Показывать в виде дерева**.
3. Откройте контекстное меню узла **Виртуальные диски**.
4. Выберите пункт **Добавить виртуальный диск**.
5. В списке доступных имен выберите имя создаваемого виртуального диска.
6. Установите флажок рядом с диском, чтобы включить его в область защиты.
7. В окне **Настройка области защиты** нажмите на кнопку **Сохранить**.

Настроенные параметры будут сохранены.

Чтобы включить в область защиты виртуальную папку или виртуальный файл, выполните следующие действия:

1. Откройте окно **Настройка области защиты**.
2. В раскрывающемся списке в левом верхнем углу окна выберите пункт **Показывать в виде дерева**.
3. Откройте контекстное меню виртуального диска, в который вы хотите добавить папку или файл, и выберите один из следующих пунктов:
   - **Добавить виртуальную папку**, чтобы добавить виртуальную папку в область защиты.
   - **Добавить виртуальный файл**, чтобы добавить виртуальный файл в область защиты.
4. В поле ввода задайте имя папки или файла.
5. В строке с именем созданной папки или созданного файла установите флажок, чтобы включить папку или файл в область защиты.
6. В окне **Настройка области защиты** нажмите на кнопку **Сохранить**.

Настроенные изменения параметров задачи будут сохранены.

Настройка параметров безопасности вручную

По умолчанию в задачах постоянной защиты компьютера применяются единые параметры безопасности для всей области защиты. Эти параметры соответствуют стандартному уровню безопасности **Рекомендуемый**.

Можно изменять значения параметров безопасности, заданные по умолчанию, настроив их как едиными для всей области защиты, так и различными для отдельных элементов в дереве или списке файловых ресурсов устройства.

При работе с деревом файловых ресурсов защищаемого устройства параметры безопасности, настроенные для выбранного родительского узла, автоматически применяются для всех вложенных узлов. Параметры безопасности родительского узла не применяются к вложенному узлу, который настраивается отдельно.

Чтобы настроить параметры безопасности вручную, выполните следующие действия:

1. Откройте окно **Настройка области защиты**.
2. В левой части окна выберите узел, параметры безопасности которого вы хотите настроить.

   К выбранному в области защиты узлу или элементу можно применить стандартный шаблон параметров безопасности.

   В левой части окна можно выбрать тип отображения сетевых файловых ресурсов, создать область защиты и создать виртуальную область защиты.
3. В правой части окна выполните одно из следующих действий:
   - На закладке **Уровень безопасности** выберите требуемый уровень безопасности.
   - На следующих закладках настройте параметры безопасности выбранного узла или элемента в соответствии с вашими требованиями:
     - **Общие**
     - **Действия**
     - **Производительность**
4. В окне **Настройка области защиты** нажмите на кнопку **Сохранить**.

Новые параметры области защиты будут сохранены.

Выбор стандартных уровней безопасности в задаче Постоянная защита файлов

Для выбранных в дереве или списке файловых ресурсов защищаемого устройства узлов можно задать один из следующих стандартных уровней безопасности: **Максимальное быстродействие**, **Рекомендуемый** и **Максимальная защита**.

Чтобы выбрать один из стандартных уровней безопасности, выполните следующие действия:

1. Откройте окно **Настройка области защиты**.
2. В дереве или в списке сетевых файловых ресурсов защищаемого устройства выберите узел или элемент, для которого вы хотите задать стандартный уровень безопасности.
3. Убедитесь, что выбранный узел или элемент включен в область защиты.
4. В правой части окна на закладке **Уровень безопасности** выберите требуемый уровень безопасности.

   В окне отобразится список значений параметров безопасности, соответствующих выбранному уровню безопасности.
5. Нажмите на кнопку **Сохранить**.

   Параметры задачи будут сохранены и применены немедленно в выполняющейся задаче. Если задача не выполняется, измененные параметры будут применены при ее следующем запуске.

Настройка общих параметров задачи

Чтобы настроить общие параметры безопасности задачи Постоянная защита файлов, выполните следующие действия.

1. Откройте окно **Настройка области защиты**.
2. Выберите закладку **Общие**.
3. В блоке **Защита объектов** укажите объекты, которые требуется включить в область защиты:
   - **Все объекты**
   - **Объекты, проверяемые по формату**
   - **Объекты, проверяемые по списку расширений, указанному в антивирусных базах**
   - **Объекты, проверяемые по указанному списку расширений**
   - **Загрузочные секторы дисков и MBR**
   - **Альтернативные потоки NTFS**
4. В блоке параметров **Оптимизация** установите или снимите флажок **Проверка только новых и измененных файлов**.

   Для переключения между доступными вариантами при снятом флажке перейдите по ссылке **Все** / **Только новые** для каждого типа составных объектов.

5. В блоке **Защита составных объектов** укажите составные объекты, которые вы хотите включить в область защиты:
   - **Все** / **Только новые архивы**
   - **Все** / **Только новые SFX-архивы**
   - **Все** / **Только новые почтовые базы**
   - **Все** / **Только новые упакованные объекты**
   - **Все** / **Только новые файлы почтовых форматов**
   - **Все** / **Только новые вложенные OLE-объекты**
6. Нажмите на кнопку **Сохранить**.

Новая конфигурация задачи будет сохранена.

Настройка действий

Чтобы настроить действия, которые задача Постоянная защита файлов выполняет над зараженными и другими обнаруженными объектами, выполните следующие действия:

1. Откройте окно **Настройка области защиты**.
2. Выберите закладку **Действия**.
3. Выберите действие над зараженными и другими обнаруживаемыми объектами:
   - **Только сообщать**
   - **Блокировать доступ**
   - **Выполнять дополнительное действие**

     Выберите действие из раскрывающегося списка:
     - **Лечить**
     - **Лечить. Удалять, если лечение невозможно**
     - **Удалять**
     - **Рекомендуемое**
4. Выберите действие над возможно зараженными объектами:
   - **Только сообщать**
   - **Блокировать доступ**
   - **Выполнять дополнительное действие**

     Выберите действие из раскрывающегося списка:
     - **Помещать на карантин**
     - **Удалять**
     - **Рекомендуемое**
5. Настройте действия над объектами в зависимости от типа обнаруженного объекта:
   a. Снимите или установите флажок **Выполнять действия в зависимости от типа обнаруженного объекта**.
   b. Нажмите на кнопку **Настройка**.
   c. В открывшемся окне выберите первичное действие и (на случай неудачного выполнения первичного действия) вторичное действие для каждого типа обнаруженного объекта.
   d. Нажмите на кнопку **ОК**.
6. Выберите действие над неизменяемыми составными файлами: снимите или установите флажок **Полностью удалять составной файл при обнаружении вложенного объекта, если составной файл не может быть изменен программой**.
7. Нажмите на кнопку **Сохранить**.

Новая конфигурация задачи будет сохранена.

Настройка производительности

Чтобы настроить параметры производительности задачи Постоянная защита файлов, выполните следующие действия:

1. Откройте окно **Настройка области защиты**.
2. Выберите закладку **Производительность**.
3. В блоке **Исключения**:
   - Снимите или установите флажок **Исключать файлы**.
   - Снимите или установите флажок **Не обнаруживать**.
   - Нажмите на кнопку **Изменить** для каждого параметра, чтобы добавить исключения.
4. В блоке **Дополнительные параметры**:
   - **Останавливать проверку, если она длится более (сек.)**
   - **Не проверять составные объекты размером более (МБ)**
   - **Использовать технологию iSwift**
   - **Использовать технологию iChecker**

Статистика задачи Постоянная защита файлов

Пока выполняется задача Постоянная защита файлов, вы можете просматривать в реальном времени информацию о количестве объектов, обработанных Kaspersky Embedded Systems Security с момента запуска задачи.

Чтобы просмотреть статистику задачи Постоянная защита файлов, выполните следующие действия:

1. В дереве Консоли программы разверните узел **Постоянная защита компьютера**.
2. Выберите вложенный узел **Постоянная защита файлов**.

В панели результатов выбранного узла в блоке **Статистика** отобразится статистика задачи.

Вы можете просмотреть информацию об объектах, обработанных Kaspersky Embedded Systems Security с момента запуска задачи (см. таблицу ниже).

Статистика задачи Постоянная защита файлов

Поле	Описание
Обнаружено	Количество объектов, которые обнаружила программа Kaspersky Embedded Systems Security. Например, если программа Kaspersky Embedded Systems Security

	обнаружила один вредоносный объект в пяти файлах, значение в этом поле увеличится на единицу.
Зараженных и других обнаруживаемых объектов	Количество объектов, которые программа Kaspersky Embedded Systems Security признала зараженными, или количество обнаруженных легальных программ, которые могут быть использованы злоумышленниками для нанесения вреда устройству или персональным данным.
Возможно зараженных объектов	Количество объектов, которые программа Kaspersky Embedded Systems Security признала возможно зараженными.
Объектов не вылечено	Количество объектов, которые программа Kaspersky Embedded Systems Security не вылечила по следующим причинам: • Тип обнаруженного объекта не предполагает лечения. • При лечении возникла ошибка.
Объектов не помещено на карантин	Количество объектов, которые программе Kaspersky Embedded Systems Security не удалось поместить на карантин, например, из-за отсутствия свободного места на диске.
Объектов не удалено	Количество объектов, которые программе Kaspersky Embedded Systems Security не удалось удалить, например, если доступ к объекту был заблокирован другой программой.
Объектов не проверено	Количество объектов в области защиты, которые программе Kaspersky Embedded Systems Security не удалось проверить, например, если доступ к объекту был заблокирован другой программой.
Объектов, не помещенных в резервное хранилище	Количество объектов, копии которых программе Kaspersky Embedded Systems Security не удалось сохранить в резервном хранилище, например, из-за отсутствия свободного места на диске.
Ошибок обработки	Количество объектов, во время обработки которых возникла ошибка задачи.
Вылечено объектов	Количество объектов, которые вылечила программа Kaspersky Embedded Systems Security.
Помещено на карантин	Количество объектов, которые программа Kaspersky Embedded Systems Security поместила на карантин.
Помещено в резервное хранилище	Количество объектов, копии которых программа Kaspersky Embedded Systems Security сохранила в резервном хранилище.
Удалено объектов	Количество объектов, которые удалила программа Kaspersky Embedded Systems Security.
Защищенных паролем объектов	Количество объектов (например, архивов), которые программа Kaspersky Embedded Systems Security пропустила, так как эти объекты защищены паролем.
Поврежденных объектов	Количество объектов, которые программа Kaspersky Embedded Systems Security пропустила, так как их формат искажен.
Обработано объектов	Общее количество объектов, которые обработала программа Kaspersky Embedded Systems Security.

Вы также можете посмотреть статистику задачи Постоянная защита файлов в журнале выполнения задачи по ссылке **Открыть журнал выполнения** в разделе **Управление** панели результатов.

Если значение в поле **Всего событий:** в окне журнала выполнения задачи Постоянная защита файлов больше 0, рекомендуется вручную обработать события в журнале выполнения задачи на закладке **События**.

Управление задачей Постоянная защита файлов с помощью Веб-плагина

С помощью Веб-плагина нельзя изменить стандартный уровень безопасности для задачи Постоянная защита файлов.

Чтобы настроить задачу Постоянная защита файлов с помощью Веб-плагина, выполните следующие действия:

1. В главном окне веб-консоли выберите **Устройства** → **Политики и профили**.
2. Выберите политику, которую вы хотите настроить.
3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.
4. Перейдите в раздел **Постоянная защита компьютера**.
5. Нажмите на кнопку **Параметры** в подразделе **Постоянная защита файлов**.
6. Настройте параметры, приведены в следующей таблице.

Параметры задачи Постоянная защита файлов

Параметр	Описание
Интеллектуальный режим	Kaspersky Embedded Systems Security выбирает объекты для проверки самостоятельно. Объект проверяется при открытии и повторно после сохранения, если объект был изменен. Если процесс многократно обращается к объекту и изменяет его, Kaspersky Embedded Systems Security повторно проверяет объект только после его последнего сохранения этим процессом.
При открытии	Kaspersky Embedded Systems Security проверяет все объекты при их открытии на чтение, выполнение и изменение.
При открытии и изменении	Kaspersky Embedded Systems Security проверяет объект при открытии, а затем повторно при сохранении, если объект был изменен. Этот вариант выбран по умолчанию.
При выполнении	Kaspersky Embedded Systems Security проверяет файл только при открытии на выполнение.
Использовать эвристический анализатор	Флажок включает или выключает использование эвристического анализатора при проверке объектов. Если флажок установлен, эвристический анализатор включен. Если флажок снят, эвристический анализатор выключен. По умолчанию флажок установлен.

Уровень эвристического анализа	Уровень эвристического анализа обеспечивает баланс между тщательностью поиска угроз, степенью загрузки ресурсов операционной системы и временем проверки. Существуют следующие уровни чувствительности проверки: • **Поверхностный**. Эвристический анализатор выполняет меньше инструкций, содержащихся в исполняемых файлах. При таком режиме вероятность обнаружить угрозу снижается. Проверка требует меньше ресурсов системы и выполняется быстрее. • **Средний**. Эвристический анализатор выполняет то количество инструкций в исполняемом файле, которое рекомендовано специалистами "Лаборатории Касперского". Этот уровень выбран по умолчанию. • **Глубокий**. Эвристический анализатор выполняет больше инструкций, содержащихся в исполняемых файлах. При таком режиме вероятность обнаружить угрозу возрастает. Проверка требует больше ресурсов системы, занимает больше времени, а также возможно увеличение количества ложных срабатываний. Параметр доступен, если установлен флажок **Использовать эвристический анализатор**.
Применять доверенную зону	Флажок включает или выключает применение доверенной зоны в работе задачи. Если флажок установлен, Kaspersky Embedded Systems Security добавляет к исключениям из проверки, установленным при настройке параметров задачи, файловые операции доверенных процессов. Если флажок снят, Kaspersky Embedded Systems Security не учитывает файловые операции доверенных процессов при формировании области защиты для задачи. По умолчанию флажок установлен.
Использовать KSN для защиты	Этот флажок включает или выключает использование служб KSN. Если флажок установлен, программа использует данные Kaspersky Security Network, что обеспечивает более высокую скорость реакции программы на новые угрозы и снижает вероятность ложных срабатываний. Если флажок снят, задача не использует службы KSN. По умолчанию флажок установлен.
Блокировать доступ к сетевым файловым ресурсам для узлов, с которых ведется вредоносная активность	Флажок включает или выключает добавление узлов, со стороны которых выявлена вредоносная активность, в список заблокированных узлов. Если флажок установлен, Kaspersky Embedded Systems Security добавляет узлы, со стороны которых выявлена вредоносная активность, в список заблокированных узлов. Если флажок снят, Kaspersky Embedded Systems Security не добавляет узлы, со стороны которых выявлена вредоносная активность, в список заблокированных узлов. По умолчанию флажок снят. Список заблокированных узлов можно просмотреть в хранилище заблокированных узлов.

	Можно восстановить доступ к заблокированным узлам, а также указать количество суток, часов и минут, по истечении которых с момента блокировки узлы получают доступ к сетевым файловым ресурсам, настроив параметры хранилища заблокированных узлов.
Запустить сканирование важных областей при обнаружении активного заражения	Если этот флажок установлен, то при обнаружении активного заражения Kaspersky Embedded Systems Security создает и запускает временную задачу Проверка важных областей. После завершения выполнения временной задачи Проверка важных областей, Kaspersky Embedded Systems Security удаляет эту временную задачу. Если флажок не установлен, то при обнаружении активного заражения Kaspersky Embedded Systems Security не создает и не запускает задачу Проверка важных областей. По умолчанию флажок установлен.
Область защиты	Можно настроить параметры безопасности для области защиты.

Использование KSN

Этот раздел содержит информацию о задаче Использование KSN и инструкции о том, как настроить параметры этой задачи.

О задаче Использование KSN

Kaspersky Security Network (далее также "KSN") – это инфраструктура онлайн-служб, предоставляющая доступ к оперативной базе знаний "Лаборатории Касперского" о репутации файлов, веб-ресурсов и программ. Использование данных Kaspersky Security Network обеспечивает более высокую скорость реакции Kaspersky Embedded Systems Security на новые угрозы, повышает эффективность работы некоторых компонентов защиты, а также снижает вероятность ложных срабатываний.

Для запуска задачи Использование KSN необходимо принять Положение о Kaspersky Security Network.

Kaspersky Embedded Systems Security получает от Kaspersky Security Network только информацию о репутации программ.

Участие пользователей в KSN позволяет "Лаборатории Касперского" оперативно получать информацию о типах и источниках новых угроз, разрабатывать способы их нейтрализации, уменьшать количество ложных срабатываний компонентов программы.

Более подробная информация о передаче, обработке, хранении и уничтожении информации об использовании программы приведена в окне **Обработка данных** задачи Использование KSN и в Политике конфиденциальности на веб-сайте "Лаборатории Касперского".

Участие в Kaspersky Security Network добровольное. Решение об участии в Kaspersky Security Network принимается после установки Kaspersky Embedded Systems Security. Вы можете изменить свое решение об участии в Kaspersky Security Network в любой момент.

Kaspersky Security Network можно использовать в следующих задачах Kaspersky Embedded Systems Security:

- Постоянная защита файлов.
- Проверка по требованию.
- Контроль запуска программ.

Kaspersky Private Security Network

Подробнее о том, как настроить Kaspersky Private Security Network (далее также "Локальный KSN"), см. в *Справке Kaspersky Security Center*.

Если вы используете Локальный KSN на устройстве, в окне **Обработка данных** задачи Использование KSN можно ознакомиться с Положением о KSN и включить использование компонента, установив флажок **Я принимаю условия Положения о Kaspersky Security Network**. Принимая условия, вы соглашаетесь отправлять все типы данных, упомянутые в Положении о KSN (запросы безопасности, статистические данные), в службы KSN.

После принятия условий Локального KSN флажки, регулирующие использование Глобального KSN, недоступны.

Если вы отключаете Локальный KSN во время выполнения задачи Использование KSN, происходит ошибка *Нарушение лицензии* и выполнение задачи прекращается. Чтобы продолжить защищать устройство, вам нужно принять Положение о KSN в окне **Обработка данных** и перезапустить задачу.

Отзыв согласия с Положением о KSN

Вы можете отозвать свое согласие и прекратить обмен данными с Kaspersky Security Network в любой момент. Следующие действия считаются полным или частичным отзывом согласия с Положением о KSN:

- Вы сняли флажок **Разрешить отправку данных о проверяемых файлах**: программа перестает отправлять контрольные суммы проверенных файлов в службу KSN для анализа.
- Вы сняли флажок **Разрешить отправку статистики Kaspersky Security Network**: программа прекращает обрабатывать данные с дополнительной статистикой KSN.
- Вы сняли флажок **Я принимаю условия Положения о Kaspersky Security Network**: программа прекращает обрабатывать все связанные с KSN данные, задача Использование KSN останавливается.
- Вы удалили компонент Использование KSN: обработка всех связанных с KSN данных останавливается.
- Вы удалили Kaspersky Embedded Systems Security: обработка всех связанных с KSN данных останавливается.

Параметры по умолчанию для задачи Использование KSN

Вы можете изменять параметры задачи Использование KSN, заданные по умолчанию (см. таблицу ниже).

Параметры по умолчанию для задачи Использование KSN

Параметр	Значение по умолчанию	Описание
Действия над объектами, недоверенными в KSN	Удалить	Вы можете указывать действия, которые Kaspersky Embedded Systems Security будет выполнять над объектами, имеющими репутацию недоверенных в KSN.
Отправка данных	Контрольная сумма файла (MD5-хеш) рассчитывается для файлов, размер которых не превышает 2 МБ.	Вы можете указывать максимальный размер файлов, для которых рассчитывается контрольная сумма по алгоритму MD5 для отправки в KSN. Если флажок снят, Kaspersky Embedded Systems Security рассчитывает MD5-хеш для файлов любого размера.
Расписание	Время первого запуска	Вы можете запустить задачу вручную или настроить запуск

запуска задачи	не задано.	задачи по расписанию.
Использовать Kaspersky Security Center в качестве прокси-сервера KSN	Выбрано.	По умолчанию все данные отправляются в KSN через Kaspersky Security Center. Этот параметр можно изменять только с помощью Плагина управления.
Я принимаю условия Положения о Kaspersky Security Network	Флажок снят	Если флажок установлен, от вас получено согласие на участие в KSN после установки программы. Вы можете изменить свое решение в любой момент.
Разрешить отправку статистики Kaspersky Security Network	Установлен (применяется, только если принято Положение о KSN).	Если вы приняли Положение о KSN, статистика будет отправляться автоматически, пока вы не снимете флажок.
Разрешить отправку данных о проверяемых файлах	Установлен (применяется, только если принято Положение о KSN).	Если Положение о KSN принято, данные о файлах, которые были проверены и проанализированы с момента запуска задачи, отправляются. Снять флажок можно в любой момент.
Принять условия Положения о Kaspersky Managed Protection	Флажок снят	Вы можете включать и выключать службу KMP. Служба доступна, только если во время приобретения программы был подписан дополнительный договор.

Управление использованием KSN с помощью Плагина управления

В этом разделе описана настройка использования KSN и обработки данных с помощью Плагина управления.

Настройка параметров задачи Использование KSN

Чтобы настроить задачу Использование KSN, выполните следующие действия:

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.

2. Выберите группу администрирования, для которой требуется настроить параметры программы.

3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:

   - Чтобы настроить параметры программы для группы защищаемых устройств, выберите закладку **Политики** и откройте окно **Свойства: <Имя политики>**.

- Чтобы настроить параметры программы для отдельного защищаемого устройства, выберите закладку **Устройства** и откройте окно **Параметры программы**.

  Если к устройству применяется активная политика Kaspersky Security Center, запрещающая изменение параметров программы, эти параметры недоступны для изменения в окне **Параметры программы**.

4. В разделе **Постоянная защита компьютера** нажмите на кнопку **Настройка** в подразделе **Использование KSN**.

   Откроется окно **Использование KSN**.

5. На закладке **Общие** настройте следующие параметры задачи:

   - В разделе **Действия над объектами, недоверенными в KSN** укажите действие, которое выполняет Kaspersky Embedded Systems Security при обнаружении объекта, имеющего репутацию недоверенного в KSN:

     - **Удалять**
     - **Фиксировать информацию в отчете**

   - В разделе **Отправка данных** ограничьте размер файлов, для которых вычисляется контрольная сумма:

     - Снимите или установите флажок **Не рассчитывать контрольную сумму для отправки в KSN, если размер файла превышает (МБ)**.
     - Если требуется, в поле справа измените значение максимального размера файлов, для которых Kaspersky Embedded Systems Security будет рассчитывать контрольную сумму.

   - В разделе **Прокси-сервер KSN** снимите или установите флажок **Использовать Kaspersky Security Center в качестве прокси-сервера KSN**.

     Чтобы включить прокси-сервер KSN, необходимо принять Положение о KSN и настроить Kaspersky Security Center. Подробнее см. в *Справке Kaspersky Security Center*.

6. Если требуется, настройте расписание запуска задачи на закладке **Управление задачей**. Например, вы можете настроить запуск задачи по расписанию и указать частоту запуска задачи **При запуске программы**, если вы хотите, чтобы задача автоматически запускалась после перезагрузки защищаемого устройства.

   Программа будет запускать задачу Использование KSN по расписанию.

7. Перед запуском задачи настройте обработку данных.

8. Нажмите на кнопку **ОК**.

Изменения параметров задачи будут применены. Дата и время изменения параметров, а также информация о параметрах задачи до и после их изменения будут сохранены в журнале системного аудита.

Настройка обработки данных

Чтобы настроить типы данных, которые будут обрабатываться службами KSN, и принять Положение о KSN, выполните следующие действия:

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.

2. Выберите группу администрирования, для которой требуется настроить параметры программы.

3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:

   - Чтобы настроить параметры программы для группы защищаемых устройств, выберите закладку **Политики** и откройте окно **Свойства: <Имя политики>**.

   - Чтобы настроить параметры программы для отдельного защищаемого устройства, выберите закладку **Устройства** и откройте окно **Параметры программы**.

     Если к устройству применяется активная политика Kaspersky Security Center, запрещающая изменение параметров программы, эти параметры недоступны для изменения в окне **Параметры программы**.

4. В разделе **Постоянная защита компьютера** нажмите на кнопку **Обработка данных** в подразделе **Использование KSN**.

   Откроется окно **Обработка данных в KSN**.

5. На закладке **Службы и статистика KSN** прочитайте текст Положения и установите флажок **Я принимаю условия Положения о Kaspersky Security Network**.

6. Для повышения уровня защиты, следующие флажки установлены по умолчанию:

   - **Разрешить отправку данных о проверяемых файлах**

   - **Разрешить отправку статистики Kaspersky Security Network**

   Вы можете снять флажки и прекратить передачу дополнительных данных в любой момент.

7. На закладке **Kaspersky Managed Protection** ознакомьтесь с Положением и установите флажок **Принять условия Положения о Kaspersky Managed Protection**.

   При изменении состояния флажка **Принять условия Положения о Kaspersky Managed Protection** не происходит немедленный запуск или остановка обработки данных. Для того чтобы изменения вступили в силу, необходимо перезапустить Kaspersky Embedded Systems Security.

   Для использования службы KMP необходимо подписать соответствующее соглашение и запустить исполнение конфигурационных файлов на защищаемом устройстве.

   Для использования службы KMP необходимо принять условия обработки данных Положения о KSN на закладке **Службы и статистика KSN**.

8. Нажмите на кнопку **OK**.

   Конфигурация обработки данных будет сохранена.

Управление использованием KSN с помощью Консоли программы

В этом разделе описана настройка использования KSN и обработки данных с помощью Консоли программы.

Настройка параметров задачи Использование KSN

Чтобы настроить задачу Использование KSN, выполните следующие действия:

1. В дереве Консоли программы разверните узел **Постоянная защита компьютера**.
2. Выберите вложенный узел **Использование KSN**.
3. В панели результатов перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи** на закладке **Общие**.
4. Настройте параметры задачи:
   - В разделе **Действия над объектами, недоверенными в KSN** укажите действие, которое выполняет Kaspersky Embedded Systems Security при обнаружении объекта, имеющего репутацию недоверенного в KSN:
     - **Удалять**
     - **Фиксировать информацию в отчете**
   - В разделе **Отправка данных** ограничьте размер файлов, для которых вычисляется контрольная сумма:
     - Снимите или установите флажок **Не рассчитывать контрольную сумму для отправки в KSN, если размер файла превышает (МБ)**.
     - Если требуется, в поле справа измените значение максимального размера файлов, для которых Kaspersky Embedded Systems Security будет рассчитывать контрольную сумму.
5. Если требуется, настройте расписание запуска задачи на закладках **Расписание** и **Дополнительно**. Например, вы можете настроить запуск задачи по расписанию и указать частоту запуска задачи **При запуске программы**, если вы хотите, чтобы задача автоматически запускалась после перезагрузки защищаемого устройства.

   Программа будет запускать задачу Использование KSN по расписанию.
6. Перед запуском задачи настройте обработку данных.
7. Нажмите на кнопку **ОК**.

Изменения параметров задачи будут применены. Дата и время изменения параметров, а также информация о параметрах задачи до и после их изменения будут сохранены в журнале системного аудита.

Настройка обработки данных

Чтобы настроить типы данных, которые будут обрабатываться службами KSN, и принять Положение о KSN, выполните следующие действия:

1. В дереве Консоли программы разверните узел **Постоянная защита компьютера**.
2. Выберите вложенный узел **Использование KSN**.
3. В панели результатов перейдите по ссылке **Обработка данных**.

   Откроется окно **Обработка данных**.
4. На закладке **Службы и статистика KSN** прочитайте текст Положения и установите флажок **Я принимаю условия Положения о Kaspersky Security Network**.
5. Для повышения уровня защиты, следующие флажки установлены по умолчанию:

   - **Разрешить отправку данных о проверяемых файлах**
   - **Разрешить отправку статистики Kaspersky Security Network**

   Вы можете снять флажки и прекратить передачу дополнительных данных в любой момент.
6. На закладке **Kaspersky Managed Protection** ознакомьтесь с Положением и установите флажок **Принять условия Положения о Kaspersky Managed Protection**.

   При изменении состояния флажка **Принять условия Положения о Kaspersky Managed Protection** не происходит немедленный запуск или остановка обработки данных. Для того чтобы изменения вступили в силу, необходимо перезапустить Kaspersky Embedded Systems Security.

   Для использования службы KMP необходимо подписать соответствующее соглашение и запустить исполнение конфигурационных файлов на защищаемом устройстве.

   Для использования службы KMP необходимо принять условия обработки данных Положения о KSN на закладке **Службы и статистика KSN**.
7. Нажмите на кнопку **OK**.

Конфигурация обработки данных будет сохранена.

Управление использованием KSN с помощью Веб-плагина

Чтобы настроить использование KSN и обработку данных с помощью Веб-плагина, выполните следующие действия:

1. В главном окне веб-консоли выберите **Устройства** → **Политики и профили**.
2. Выберите политику, которую вы хотите настроить.
3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.
4. Перейдите в раздел **Постоянная защита компьютера**.

5. Нажмите на кнопку **Параметры** в подразделе **Использование KSN**.

6. Настройте параметры, приведены в следующей таблице.

Настройка параметров задачи Использования KSN и обработки данных с помощью Плагина управления

Параметр	Описание
Удалить	Kaspersky Embedded Systems Security удаляет недоверенный по данным KSN объект и помещает его копию в резервное хранилище. Этот вариант выбран по умолчанию.
Фиксировать информацию в отчете	Kaspersky Embedded Systems Security фиксирует в журнале выполнения задач информацию об обнаруженном недоверенном по данным KSN объекте. Kaspersky Embedded Systems Security не удаляет недоверенный объект.
Не рассчитывать контрольную сумму для отправки в KSN, если размер файла превышает (МБ)	Флажок включает или выключает расчет контрольной суммы файлов установленного размера для отправки этой информации в службы KSN. Продолжительность расчета контрольной суммы зависит от размера файла. Если флажок установлен, Kaspersky Embedded Systems Security не рассчитывает контрольную сумму для файлов, размер которых превышает установленное значение (в МБ). Если флажок снят, Kaspersky Embedded Systems Security рассчитывает контрольную сумму для файлов любого размера. По умолчанию флажок установлен.
Я принимаю условия Положения о Kaspersky Security Network	Устанавливая этот флажок, вы подтверждаете, что прочитали и принимаете условия Положения о Kaspersky Security Network.
Отправка данных о проверяемых файлах	Если флажок установлен, Kaspersky Embedded Systems Security отправляет контрольные суммы проверенных файлов в "Лабораторию Касперского". Заключение о безопасности каждого файла основано на репутации, полученной от KSN. Если флажок снят, Kaspersky Embedded Systems Security не отправляет контрольные суммы файлов в KSN. Обратите внимание, что запросы репутации файлов могут отправляться в ограниченном режиме. Ограничения вводятся для защиты репутационных серверов "Лаборатории Касперского" от DDoS-атак. В этом режиме параметры отправляемых запросов о репутации файлов определяются на основании правил и методов, разработанных экспертами "Лаборатории Касперского", и не могут быть изменены пользователями на защищаемом устройстве. Обновления правил и методов осуществляются в ходе выполнения задачи Обновление баз программы. Если применяется ограниченный режим, в статистике задачи Использование KSN отображается статус *применено "Лабораторией Касперского" с целью защиты репутационных серверов от DDoS*. По умолчанию флажок установлен.
Отправка данных о проверяемых файлах	Если флажок установлен, Kaspersky Embedded Systems Security отправляет дополнительную статистику, которая может содержать персональные данные. Список данных, отправляемых в качестве статистики KSN, указан в Положении о KSN. Данные, полученные "Лабораторией Касперского", используются для улучшения качества программ и повышения скорости обнаружения угроз. Если флажок снят, Kaspersky Embedded Systems Security не отправляет дополнительную статистику.

	По умолчанию флажок установлен.
Я принимаю условия Положения о Kaspersky Managed Protection	Если флажок установлен, вы соглашаетесь отправлять статистику активности защищаемого устройства специалистам "Лаборатории Касперского". Полученные данные используются для круглосуточного анализа и отчетности, необходимых для предотвращения нарушений безопасности. По умолчанию флажок снят.
Управление задачами	Вы можете настроить расписание запуска задачи.

Настройка передачи дополнительных данных

В Kaspersky Embedded Systems Security можно настроить отправку в "Лабораторию Касперского" следующих данных:

- контрольных сумм проверенных файлов (флажок **Разрешить отправку данных о проверяемых файлах**);
- дополнительной статистики, включая персональные данные (флажок **Разрешить отправку статистики Kaspersky Security Network**).

Подробнее о данных, отправляемых в "Лабораторию Касперского", см. в разделе "Локальная обработка данных" этого руководства.

Соответствующие флажки можно установить или снять, только если установлен флажок **Я принимаю условия Положения о Kaspersky Security Network**.

По умолчанию Kaspersky Embedded Systems Security отправляет контрольные суммы файлов и дополнительную статистику после принятия Положения о KSN.

Состояние флажка **Я принимаю условия Положения о Kaspersky Security Network** невозможно изменить, если политика Kaspersky Security Center запрещает изменение параметров, связанных с обработкой данных.

Возможные состояния флажков и соответствующие условия

Состояние флажка	Условия для состояния флажка Разрешить отправку данных о проверяемых файлах	Условия для состояния флажка Разрешить отправку статистики Kaspersky Security Network	Условия для состояния флажка Принять условия Положения о Kaspersky Managed Protection	Условия для состояния флажка Я принимаю условия Положения о Kaspersky Security Network
☑	• отправляются запросы репутации • действия с флажком доступны	• отправляется дополнительная статистика • действия с флажком доступны	• принимаются условия Положения о Kaspersky Managed Protection • действия с флажком доступны	• принимаются условия Положения о Kaspersky Security Network • действия с флажком доступны

☑	• отправляются запросы репутации • действия с флажком недоступны	• отправляется дополнительная статистика • действия с флажком недоступны	• принимаются условия Положения о Kaspersky Managed Protection • действия с флажком недоступны	• принимаются условия Положения о Kaspersky Security Network • действия с флажком недоступны
☐	• не отправляются запросы репутации • действия с флажком доступны	• не отправляется дополнительная статистика • действия с флажком доступны	• не принимаются условия Положения о Kaspersky Managed Protection • действия с флажком доступны	• не принимаются условия Положения о Kaspersky Security Network • действия с флажком доступны
☐	• не отправляются запросы репутации • действия с флажком недоступны	• не отправляется дополнительная статистика • действия с флажком недоступны	• не принимаются условия Положения о Kaspersky Managed Protection • действия с флажком недоступны	• не принимаются условия Положения о Kaspersky Security Network • действия с флажком недоступны

Статистика задачи Использование KSN

Пока выполняется задача Использование KSN, вы можете просматривать в реальном времени информацию о количестве объектов, которые программа Kaspersky Embedded Systems Security обработала с момента ее запуска до текущего момента. Информация обо всех событиях, произошедших во время выполнения задачи, регистрируется в журнале выполнения задачи.

Чтобы просмотреть статистику задачи Использование KSN, выполните следующие действия:

1. В дереве Консоли программы разверните узел **Постоянная защита компьютера**.
2. Выберите вложенный узел **Использование KSN**.

В панели результатов выбранного узла в блоке **Статистика** отобразится статистика задачи.

Вы можете просмотреть информацию об объектах, которые программа Kaspersky Embedded Systems Security обработала за время выполнения задачи (см. таблицу ниже).

Поле	Описание
Ошибки отправки запросов	Количество запросов в KSN, во время обработки которых возникла ошибка задачи.
Пакетов статистик сформировано	Количество пакетов с данными, которые были отправлены на обработку в KSN.
Удалено объектов	Количество объектов, которые программа Kaspersky Embedded Systems Security удалила в результате выполнения задачи Использование KSN.
Помещено в резервное хранилище	Количество объектов, копии которых программа Kaspersky Embedded Systems Security сохранила в резервном хранилище.
Объектов не удалено	Количество объектов, которые программа Kaspersky Embedded Systems Security попыталась удалить, но безуспешно, например, если доступ к объекту был заблокирован другой программой. Информация о таких объектах записывается в журнал выполнения задачи.
Объектов, не помещенных в резервное хранилище	Количество объектов, копии которых программа Kaspersky Embedded Systems Security попыталась сохранить в резервном хранилище, но безуспешно, например, из-за отсутствия доступного пространства на диске. Программа не лечит и не удаляет файлы, которые не удалось поместить в резервное хранилище. Информация о таких объектах записывается в журнал выполнения задачи.
Ограниченный режим	Статус отправки запросов файловой репутации в ограниченном режиме. В ограниченном режиме Kaspersky Embedded Systems Security отправляет только часть запросов о репутации файлов, в соответствии с рекомендациями специалистов "Лаборатории Касперского".

Защита от сетевых угроз

Этот раздел содержит информацию о задаче Защита от сетевых угроз и инструкции о том, как настроить параметры этой задачи.

О задаче Защита от сетевых угроз

Защиту от сетевых угроз можно установить только на устройства с операционной системой Microsoft Windows 7 и более поздних версий или Windows Server 2008 R2 и более поздних версий.

Задача Защита от сетевых угроз выполняет проверку входящего сетевого трафика на наличие действий, характерных для сетевых атак. При обнаружении попытки сетевой атаки, нацеленной на ваш компьютер, Kaspersky Embedded Systems Security блокирует сетевую активность со стороны атакующего компьютера. На экране отображается предупреждение, сообщающее о попытке сетевой атаки и содержащее информацию об атакующем компьютере.

По умолчанию задача Защита от сетевых угроз выполняется в режиме **Блокировать соединения при обнаружении атаки**. В этом режиме Kaspersky Embedded Systems Security добавляет IP-адреса узлов, проявляющих активность, характерную для сетевых атак, в список заблокированных узлов.

Список заблокированных узлов можно просмотреть в хранилище заблокированных узлов.

Можно восстановить доступ к заблокированным узлам, а также указать количество суток, часов и минут, по истечении которых с момента блокировки узлы получают доступ к сетевым файловым ресурсам, настроив параметры хранилища заблокированных узлов.

IP-адреса узлов, проявляющих активность, характерную для сетевых атак, удаляются из списка заблокированных узлов в следующих случаях:

- Удалена программа Kaspersky Embedded Systems Security.
- IP-адрес удален из списка заблокированных узлов вручную.
- Истек срок блокировки узла.
- Завершилось выполнение задачи Защита от сетевых угроз и не установлен флажок **Не останавливать анализ трафика, если задача не исполняется**.
- Выключен режим **Блокировать соединения при обнаружении атаки**.

Параметры по умолчанию для задачи Защита от сетевых угроз

По умолчанию в задаче Защита от сетевых угроз используются параметры, описанные в таблице ниже. Вы можете изменять значения этих параметров.

Параметры по умолчанию для задачи Защита от сетевых угроз

Параметр	Значение по умолчанию	Описание
Режим	**Блокировать**	Задачу Защита от сетевых угроз можно запустить в одном из

работы	**соединения при обнаружении атаки**	следующих режимов: **Работать в режиме pass-through**, **Только уведомлять об обнаруженных атаках** или **Блокировать соединения при обнаружении атаки**. Флажок включает или выключает добавление узлов, проявляющих активность, характерную для сетевых атак, в список заблокированных узлов. Если выбран этот режим, Kaspersky Embedded Systems Security проверяет входящий сетевой трафик на наличие активности, характерной для сетевых атак, фиксирует в журнале события об обнаруженной активности и добавляет IP-адреса узлов, проявляющих активность, характерную для сетевых атак, в список заблокированных узлов. Этот режим выбран по умолчанию. Список заблокированных узлов можно просмотреть в хранилище заблокированных узлов. Можно восстановить доступ к заблокированным узлам, а также указать количество суток, часов и минут, по истечении которых с момента блокировки узлы получают доступ к сетевым файловым ресурсам, настроив параметры хранилища заблокированных узлов. В этом режиме Kaspersky Embedded Systems Security проверяет входящий сетевой трафик на активность, характерную для сетевых атак, фиксирует в журнале события об обнаруженной активности, но не блокирует сетевую активность со стороны атакующего компьютера. В этом режиме Kaspersky Embedded Systems Security проверяет входящий сетевой трафик на активность, характерную для сетевых атак, но не фиксирует в журнале события об обнаруженной активности и не блокирует сетевую активность со стороны атакующего компьютера. Этот режим можно использовать, например, в случае снижения производительности защищаемого устройства.
Исключения	Список исключений не используется.	Укажите области, которые вы хотите исключить из области защиты.
Параметры расписания	По умолчанию, задача Защита от сетевых угроз запускается автоматически при запуске Kaspersky Embedded Systems Security.	Можно настроить расписание.

Настройка задачи Защита от сетевых угроз с помощью Консоли программы

В этом разделе описано управление задачей Защита от сетевых угроз с помощью интерфейса Консоли программы.

Общие параметры задачи

Чтобы настроить общие параметры задачи, выполните следующие действия:

1. В дереве Консоли программы разверните узел **Постоянная защита компьютера**.
2. Выберите вложенный узел **Защита от сетевых угроз**.
3. В панели результатов узла **Защита от сетевых угроз** перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи**.
4. Выберите закладку **Общие**.
5. В разделе **Режим работы** выберите режим обработки:

   - **Работать в режиме pass-through**

     В этом режиме Kaspersky Embedded Systems Security проверяет входящий сетевой трафик на активность, характерную для сетевых атак, но не фиксирует в журнале события об обнаруженной активности и не блокирует сетевую активность со стороны атакующего компьютера.

     Этот режим можно использовать, например, в случае снижения производительности защищаемого устройства.

   - **Только уведомлять об обнаруженных атаках**

     В этом режиме Kaspersky Embedded Systems Security проверяет входящий сетевой трафик на активность, характерную для сетевых атак, фиксирует в журнале события об обнаруженной активности, но не блокирует сетевую активность со стороны атакующего компьютера.

   - **Блокировать соединения при обнаружении атаки**

Флажок включает или выключает добавление узлов, проявляющих активность, характерную для сетевых атак, в список заблокированных узлов.

Если выбран этот режим, Kaspersky Embedded Systems Security проверяет входящий сетевой трафик на наличие активности, характерной для сетевых атак, фиксирует в журнале события об обнаруженной активности и добавляет IP-адреса узлов, проявляющих активность, характерную для сетевых атак, в список заблокированных узлов.

Этот режим выбран по умолчанию.

Список заблокированных узлов можно просмотреть в хранилище заблокированных узлов.

Можно восстановить доступ к заблокированным узлам, а также указать количество суток, часов и минут, по истечении которых с момента блокировки узлы получают доступ к сетевым файловым ресурсам, настроив параметры хранилища заблокированных узлов.

6. Установите или снимите флажок **Не останавливать анализ трафика, если задача не исполняется**.

Если флажок установлен, то даже при остановке выполнения задачи Защита от сетевых угроз, Kaspersky Embedded Systems Security проверяет входящий сетевой трафик на действия, характерные для сетевых атак, и блокирует сетевую активность со стороны атакующего компьютера в выбранном режиме обработки.

Если флажок снят, то при остановке задачи Защита от сетевых угроз, Kaspersky Embedded Systems Security не проверяет входящий сетевой трафик на действия, характерные для сетевых атак, и не блокирует сетевую активность со стороны атакующего компьютера.

По умолчанию флажок снят.

7. Нажмите на кнопку **OK**.

Добавление исключений

Чтобы добавить исключения для задачи Защита от сетевых угроз, выполните следующие действия:

1. В дереве Консоли программы разверните узел **Постоянная защита компьютера**.
2. Выберите вложенный узел **Защита от сетевых угроз**.
3. В панели результатов узла **Защита от сетевых угроз** перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи**.
4. На закладке **Исключения** установите флажок **Не останавливать анализ трафика, если задача не исполняется**.

Если этот флажок установлен, Kaspersky Embedded Systems Security не проверяет входящий сетевой трафик со стороны исключенных IP-адресов.

Если флажок снят, Kaspersky Embedded Systems Security не применяет список исключений.

5. Укажите IP-адрес и нажмите на кнопку **Добавить**.
6. Нажмите на кнопку **OK**.

Настройка задачи Защита от сетевых угроз с помощью Плагина управления

В этом разделе описано управление задачей Защита от сетевых угроз с помощью интерфейса Плагина управления.

Общие параметры задачи

Чтобы настроить общие параметры задачи, выполните следующие действия:

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить параметры программы.
3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
   - Чтобы настроить параметры программы для группы защищаемых устройств, выберите закладку **Политики** и откройте окно **Свойства: <Имя политики>**.
   - Чтобы настроить параметры программы для отдельного защищаемого устройства, выберите закладку **Устройства** и откройте окно **Параметры программы**.

     Если к устройству применяется активная политика Kaspersky Security Center, запрещающая изменение параметров программы, эти параметры недоступны для изменения в окне **Параметры программы**.
4. В разделе **Постоянная защита компьютера** нажмите на кнопку **Настройка** в подразделе **Защита от сетевых угроз**.

   Откроется окно **Защита от сетевых угроз**.
5. Выберите закладку **Общие**.
6. В разделе **Режим работы** выберите режим обработки:
   - **Работать в режиме pass-through**

     В этом режиме Kaspersky Embedded Systems Security проверяет входящий сетевой трафик на активность, характерную для сетевых атак, но не фиксирует в журнале события об обнаруженной активности и не блокирует сетевую активность со стороны атакующего компьютера.

     Этот режим можно использовать, например, в случае снижения производительности защищаемого устройства.
   - **Только уведомлять об обнаруженных атаках**

В этом режиме Kaspersky Embedded Systems Security проверяет входящий сетевой трафик на активность, характерную для сетевых атак, фиксирует в журнале события об обнаруженной активности, но не блокирует сетевую активность со стороны атакующего компьютера.

- **Блокировать соединения при обнаружении атаки**

  Флажок включает или выключает добавление узлов, проявляющих активность, характерную для сетевых атак, в список заблокированных узлов.

  Если выбран этот режим, Kaspersky Embedded Systems Security проверяет входящий сетевой трафик на наличие активности, характерной для сетевых атак, фиксирует в журнале события об обнаруженной активности и добавляет IP-адреса узлов, проявляющих активность, характерную для сетевых атак, в список заблокированных узлов.

  Этот режим выбран по умолчанию.

  Список заблокированных узлов можно просмотреть в хранилище заблокированных узлов.

  Можно восстановить доступ к заблокированным узлам, а также указать количество суток, часов и минут, по истечении которых с момента блокировки узлы получают доступ к сетевым файловым ресурсам, настроив параметры хранилища заблокированных узлов.

7. Установите или снимите флажок **Не останавливать анализ трафика, если задача не исполняется**.

   Если флажок установлен, то даже при остановке выполнения задачи Защита от сетевых угроз, Kaspersky Embedded Systems Security проверяет входящий сетевой трафик на действия, характерные для сетевых атак, и блокирует сетевую активность со стороны атакующего компьютера в выбранном режиме обработки.

   Если флажок снят, то при остановке задачи Защита от сетевых угроз, Kaspersky Embedded Systems Security не проверяет входящий сетевой трафик на действия, характерные для сетевых атак, и не блокирует сетевую активность со стороны атакующего компьютера.

   По умолчанию флажок снят.

8. Нажмите на кнопку **OK**.

Добавление исключений

Чтобы добавить исключения для задачи Защита от сетевых угроз, выполните следующие действия:

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.

2. Выберите группу администрирования, для которой требуется настроить параметры программы.

3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:

   - Чтобы настроить параметры программы для группы защищаемых устройств, выберите закладку **Политики** и откройте окно **Свойства: <Имя политики>**.

   - Чтобы настроить параметры программы для отдельного защищаемого устройства, выберите закладку **Устройства** и откройте окно **Параметры программы**.

Если к устройству применяется активная политика Kaspersky Security Center, запрещающая изменение параметров программы, эти параметры недоступны для изменения в окне **Параметры программы**.

4. В разделе **Постоянная защита компьютера** нажмите на кнопку **Настройка** в подразделе **Защита от сетевых угроз**.

   Откроется окно **Защита от сетевых угроз**.

5. На закладке **Исключения** установите флажок **Не останавливать анализ трафика, если задача не исполняется**.

   Если этот флажок установлен, Kaspersky Embedded Systems Security не проверяет входящий сетевой трафик со стороны исключенных IP-адресов.

   Если флажок снят, Kaspersky Embedded Systems Security не применяет список исключений.

6. Укажите IP-адрес и нажмите на кнопку **Добавить**.

7. Нажмите на кнопку **OK**.

Настройка задачи Защита от сетевых угроз с помощью Веб-плагина

В этом разделе описано управление задачей Защита от сетевых угроз с помощью интерфейса Веб-плагина.

Общие параметры задачи

Чтобы настроить общие параметры задачи, выполните следующие действия:

1. В главном окне веб-консоли выберите **Устройства** → **Политики и профили**.
2. Выберите политику, которую вы хотите настроить.
3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.
4. Перейдите в раздел **Постоянная защита компьютера**.
5. Нажмите на кнопку **Параметры** в подразделе **Защита от сетевых угроз**.
6. Выберите закладку **Общие**.
7. В разделе **Режим работы** выберите режим обработки:

   - **Работать в режиме pass-through**

В этом режиме Kaspersky Embedded Systems Security проверяет входящий сетевой трафик на активность, характерную для сетевых атак, но не фиксирует в журнале события об обнаруженной активности и не блокирует сетевую активность со стороны атакующего компьютера.

Этот режим можно использовать, например, в случае снижения производительности защищаемого устройства.

- **Только уведомлять об обнаруженных атаках**

  В этом режиме Kaspersky Embedded Systems Security проверяет входящий сетевой трафик на активность, характерную для сетевых атак, фиксирует в журнале события об обнаруженной активности, но не блокирует сетевую активность со стороны атакующего компьютера.

- **Блокировать соединения при обнаружении атаки**

  Флажок включает или выключает добавление узлов, проявляющих активность, характерную для сетевых атак, в список заблокированных узлов.

  Если выбран этот режим, Kaspersky Embedded Systems Security проверяет входящий сетевой трафик на наличие активности, характерной для сетевых атак, фиксирует в журнале события об обнаруженной активности и добавляет IP-адреса узлов, проявляющих активность, характерную для сетевых атак, в список заблокированных узлов.

  Этот режим выбран по умолчанию.

  Список заблокированных узлов можно просмотреть в хранилище заблокированных узлов.

  Можно восстановить доступ к заблокированным узлам, а также указать количество суток, часов и минут, по истечении которых с момента блокировки узлы получают доступ к сетевым файловым ресурсам, настроив параметры хранилища заблокированных узлов.

8. Установите или снимите флажок **Не останавливать анализ трафика, если задача не исполняется**.

   Если флажок установлен, то даже при остановке выполнения задачи Защита от сетевых угроз, Kaspersky Embedded Systems Security проверяет входящий сетевой трафик на действия, характерные для сетевых атак, и блокирует сетевую активность со стороны атакующего компьютера в выбранном режиме обработки.

   Если флажок снят, то при остановке задачи Защита от сетевых угроз, Kaspersky Embedded Systems Security не проверяет входящий сетевой трафик на действия, характерные для сетевых атак, и не блокирует сетевую активность со стороны атакующего компьютера.

   По умолчанию флажок снят.

9. Нажмите на кнопку **OK**.

Добавление исключений

Чтобы добавить исключения для задачи Защита от сетевых угроз, выполните следующие действия:

1. В главном окне веб-консоли выберите **Устройства → Политики и профили**.

2. Выберите политику, которую вы хотите настроить.

3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.

4. Перейдите в раздел **Постоянная защита компьютера**.

5. Нажмите на кнопку **Параметры** в подразделе **Защита от сетевых угроз**.

6. На закладке **Исключения** установите флажок **Не останавливать анализ трафика, если задача не исполняется**.

   Если этот флажок установлен, Kaspersky Embedded Systems Security не проверяет входящий сетевой трафик со стороны исключенных IP-адресов.

   Если флажок снят, Kaspersky Embedded Systems Security не применяет список исключений.

7. Укажите IP-адрес и нажмите на кнопку **Добавить**.

8. Нажмите на кнопку **OK**.

Контроль запуска программ

Этот раздел содержит информацию о задаче Контроль запуска программ и инструкции о том, как настроить параметры этой задачи.

О задаче Контроль запуска программ

Во время выполнения задачи Контроль запуска программ Kaspersky Embedded Systems Security проверяет попытки пользователей запускать различные программы и разрешает или запрещает запуск этих программ. Задача Контроль запуска программ работает по принципу запрета по умолчанию: все программы, не указанные в качестве разрешенных в параметрах задачи, автоматически блокируются.

Вы можете разрешить запуск программ одним из следующих способов:

- задать разрешающие правила для доверенных программ;
- проверять репутацию доверенных программ в KSN при их запуске.

Запрет запуска программы имеет в задаче более высокий приоритет. Например, если запуск программы запрещен одним из правил, программа не будет запущена, независимо от заключения KSN о доверенности программы. При этом если программа признана недоверенной службами KSN, но подпадает под действие разрешающего правила, запуск такой программы будет запрещен.

Все попытки запуска программ фиксируются в журнале выполнения задач.

Задача Контроль запуска программ может выполняться в одном из двух режимов:

- **Активный** Kaspersky Embedded Systems Security с помощью набора правил контролирует запуск программ, которые попадают под действия правил контроля запуска программ. Область применения правил контроля запуска программ указывается в параметрах этой задачи. Если программа удовлетворяет правилам контроля запуска программ, а параметры задачи не удовлетворяют ни одному из указанных правил, то запуск такой программы будет запрещен.

  Запуск программ, которые не подпадают под действие правил, указанных в параметрах задачи Контроль запуска программ, разрешен, независимо от параметров задачи Контроль запуска программ.

  Задачу **Контроль запуска программ** нельзя запустить в активном режиме, если не создано ни одного правила или если для одного защищаемого устройства создано более 65535 правил.

- **Только статистика** В Kaspersky Embedded Systems Security не используются правила контроля запуска программ для запрета или разрешения запуска программ. Выполняется только запись информации обо всех запусках программ, правилах, выполненных при запуске программ, и действиях, которые были бы выполнены, если бы задача выполнялась в режиме **Активный**. Разрешен запуск всех программ. Этот режим установлен по умолчанию.

  Вы можете использовать этот режим для формирования правил контроля запуска программ на основе информации, зафиксированной в журнале выполнения задачи.

Вы можете настроить задачу Контроль запуска программ по одному из следующих сценариев:

- дополнительная настройка и применение правил контроля запуска программ;

- базовая настройка правил и использование KSN для контроля запуска программ.

Если файлы операционной системы попадают под действие задачи Контроль запуска программ, то при создании правил контроля запуска программ рекомендуется убедиться, что новые правила разрешают запуск таких программ. В противном случае операционная система может не запуститься.

Kaspersky Embedded Systems Security также перехватывает процессы, запущенные в рамках подсистемы Windows для Linux (за исключением скриптов, запущенных из оболочки UNIX™, или командных интерпретаторов). Для данных целей задача Контроль запуска программ применяет действия, указанные в текущих настройках. Задача Формирование правил контроля запуска программ фиксирует запуск программы и создает соответствующие правила для программ, работающих в рамках Windows Subsystem для Linux.

О правилах контроля запуска программ

Как работают правила контроля запуска программ

Работа правил контроля запуска программ основана на следующих составляющих:

- Тип правила.

  Правила контроля запуска программ могут разрешить или запретить запуск программы. Соответственно, они называются *разрешающими* или *запрещающими*. Для создания списка разрешающих правил контроля запуска программ можно использовать задачу формирования разрешающих правил или задачу Контроль запуска программ в режиме **Только статистика**. Можно также добавлять разрешающие правила вручную.

- Пользователь и / или группа пользователей.

  Правила контроля запуска программ контролируют запуск указанных программ пользователем или группой пользователей.

- Область применения правила.

  Правила контроля запуска программ могут применяться к *исполняемым файлам*, *скриптам* и *пакетам MSI*.

- Критерий срабатывания правила.

  Правила контроля запуска программ регулируют запуск файлов, удовлетворяющих одному из указанных в параметрах правила критериев: подписаны указанным *цифровым сертификатом*, обладают указанным *хешем SHA256* или расположены по указанному *пути*.

  Если в качестве критерия срабатывания правила выбран **Цифровой сертификат**, созданное правило контролирует запуск всех доверенных программ в операционной системе. Вы можете задать более строгие условия для этого критерия, установив следующие флажки:

  - **Использовать заголовок**
  - **Использовать отпечаток**

  Использование отпечатка наиболее строго ограничивает срабатывание правил запуска программ на основе цифрового сертификата, поскольку отпечаток является уникальным идентификатором цифрового сертификата и не может быть подделан, в отличие от заголовка цифрового сертификата.

Вы можете задать исключения для правила контроля запуска программ. Исключения из правила контроля запуска программ основываются на тех же критериях, по которым срабатывают правила: цифровой сертификат, хеш SHA256 или путь к файлу. Исключения из правил контроля запуска программ могут понадобиться для определенных разрешающих правил: например, если требуется разрешить пользователям запуск программ по пути C:\Windows, но при этом запретить запуск файла Regedit.exe.

Если файлы операционной системы попадают под действие задачи Контроль запуска программ, то при создании правил контроля запуска программ рекомендуется убедиться, что новые правила разрешают запуск таких программ. В противном случае операционная система может не запуститься.

Управление правилами контроля запуска программ

Вы можете выполнять следующие действия с правилами контроля запуска программ:

- Добавлять правила вручную.
- Формировать и добавлять правила автоматически.
- Удалять правила.
- Экспортировать правила в файл.
- Проверять выбранные файлы на наличие правил, разрешающих запуск этих файлов.
- Фильтровать список правил по заданному критерию.

О Контроле пакетов установки

Формирование правил контроля запуска программ может усложниться, если вы хотите контролировать распространение программного обеспечения на защищаемых устройствах, например, на защищаемых устройствах, где происходит регулярное автоматическое обновление установленного программного обеспечения. В этом случае требуется обновлять списки разрешающих правил после каждого обновления программного обеспечения, чтобы в параметрах задачи Контроль запуска программ учитывались новые файлы, созданные в процессе обновления. Для упрощения контроля запуска файлов в сценариях распространения программного обеспечения можно использовать подсистему Контроль пакетов установки.

Пакет установки (далее также "пакет") представляет собой программу, устанавливаемую на защищаемое устройство. В каждом пакете содержится как минимум одна программа, а также могут содержаться отдельные файлы, обновления и отдельные команды, в частности, когда выполняется установка программы или обновления.

Модуль Контроль пакетов установки реализован в виде дополнительного списка исключений. При добавлении пакета установки в список он становится доверенным. Для доверенных пакетов разрешается распаковка, а для программ, установленных или обновленных из доверенных пакетов, разрешается автоматический запуск. Извлеченные файлы могут наследовать признак доверенности от основного пакета установки. *Основной пакет установки* – это пакет, добавленный в список исключений контроля пакетов установки и ставший доверенным пакетом.

Kaspersky Embedded Systems Security контролирует только полный цикл распространения программного обеспечения. Программа не может корректно обработать запуск файлов, измененных доверенным пакетом, если при первом запуске пакета был выключен компонент Контроль пакетов установки или не был установлен компонент Контроль запуска программ.

Контроль пакетов установки невозможен, если в параметрах задачи Контроль запуска программ не установлен флажок **Использовать правила для исполняемых файлов**.

Кеш распространения программного обеспечения

Kaspersky Embedded Systems Security использует динамически формируемый кеш распространения программного обеспечения (далее "кеш распространения") для связи между доверенными пакетами и файлами, созданными во время распространения программного обеспечения. При первом запуске пакета Kaspersky Embedded Systems Security обнаруживает все файлы, созданные этим пакетом во время распространения программного обеспечения, и сохраняет контрольные суммы и пути файлов в кеше распространения. Затем, по умолчанию, разрешается запуск всех файлов в кеше распространения.

Кеш распространения нельзя просматривать, очищать и изменять вручную через пользовательский интерфейс. Kaspersky Embedded Systems Security самостоятельно наполняет и контролирует кеш.

Кеш распространения можно экспортировать в конфигурационный файл (в формате XML) и очищать с помощью команд командной строки.

Чтобы экспортировать кеш распространения в конфигурационный файл, выполните команду:

```
kavshell appcontrol /config /savetofile:<full path> /sdc
```

Чтобы полностью очистить кеш распространения, выполните команду:

```
kavshell appcontrol /config /clearsdc
```

Kaspersky Embedded Systems Security обновляет кеш распространения раз в сутки. При изменении контрольной суммы разрешенного ранее файла программа удаляет запись для этого файла из кеша распространения. При активном режиме работы задачи Контроль запуска программ дальнейшие попытки запуска этого файла будут заблокированы. При изменении полного пути к разрешенному ранее файлу последующие попытки запустить этот файл не блокируются, поскольку контрольная сумма хранится в кеше распространения.

Обработка извлеченных файлов

Все извлеченные из доверенного пакета файлы наследуют атрибут доверенности при первом запуске пакета. При снятии флажка после первого запуска все извлеченные из пакета файлы сохраняют атрибут наследования. Чтобы отменить признак наследования для всех извлеченных файлов, необходимо очистить кеш распространения и снять флажок **Разрешать дальнейшее распространение программ, созданных от этого пакета установки** перед следующим запуском доверенного пакета установки.

Извлеченные файлы и пакеты, созданные основным доверенным пакетом установки, наследуют признак доверенности, поскольку их контрольные суммы добавляются в кеш распространения, когда пакет установки из списка исключений открывается в первый раз. Таким образом, сам пакет установки и все извлеченные из него файлы являются доверенными. По умолчанию количество уровней наследования признака доверенности не ограничено.

Извлеченные файлы сохраняют признак доверенности при перезагрузке операционной системы.

Обработка файлов настраивается в параметрах Контроля пакетов установки с помощью флажка **Разрешать дальнейшее распространение программ, созданных от этого пакета установки**.

Например, если пакет test.msi, содержащий несколько пакетов и программ, добавлен в список исключений и установлен флажок, то все пакеты и программы, содержащиеся в пакете test.msi, можно распаковать и запустить, даже если они содержат другие вложенные файлы. Это соблюдается для всех уровней вложенности.

Если пакет test.msi добавлен в список исключений, а флажок **Разрешать дальнейшее распространение программ, созданных от этого пакета установки** не установлен, программа присваивает признак доверенности только пакетам и исполняемым файлам, извлеченным непосредственно из основного доверенного пакета (только первого уровня вложенности). Контрольные суммы этих файлов хранятся в кеше распространения. Все файлы второго и следующих уровней вложенности блокируются согласно принципу запрета по умолчанию.

Работа со списком правил контроля запуска программ

Список доверенных пакетов подсистемы Контроля пакетов установки – это список исключений, который дополняет, но не заменяет основной список правил контроля запуска программ.

Запрещающие правила контроля запуска программ имеют абсолютный приоритет: распаковка доверенного пакета или запуск созданных и измененных им файлов будут заблокированы, если такие пакеты и файлы подпадают под запрещающие правила контроля запуска программ.

Исключения Контроля пакетов установки учитываются и для доверенных пакетов, и для созданных и измененных ими файлов, если к таким пакетам и файлам не применяются запрещающие правила из списка правил контроля запуска программ.

Использование заключений KSN

Заключения KSN о том, что файл является недоверенным, имеют более высокий приоритет, чем исключения Контроля пакетов установки. Распаковка доверенных пакетов и запуск файлов, созданных или измененных доверенными пакетами, будет заблокирован, если для таких файлов получено заключение KSN о том, что файл является недоверенным.

При распаковке из доверенного пакета, запуск всех вложенных файлов будет разрешен, независимо от использования KSN в задаче Контроль запуска программ. При этом значение флажков **Запрещать запуск программ, недоверенных в KSN** и **Разрешать запуск программ, доверенных в KSN** не влияет на флажок **Разрешать дальнейшее распространение программ, созданных от этого пакета установки**.

Об использовании KSN в задаче Контроль запуска программ

Для запуска задачи Использование KSN необходимо принять Положение о Kaspersky Security Network.

Если данные KSN о репутации программы используются в задаче Контроль запуска программ, репутация программы по данным KSN считается основным критерием для разрешения или запрета запуска этой программы. Если KSN передает Kaspersky Embedded Systems Security данные о том, что программа не является доверенной, то попытка пользователя запустить программу блокируется. Если KSN передает Kaspersky Embedded Systems Security данные о том, что программа является доверенной, то разрешается запуск программы пользователем. KSN можно применять совместно с правилами контроля запуска программ или в качестве самостоятельного критерия блокировки запуска программ.

Применение заключений KSN в качестве самостоятельного критерия блокировки запуска программ

Этот сценарий позволяет безопасно контролировать запуски программ на защищаемом устройстве без расширенной настройки списка правил.

Вы можете применить заключения KSN к Kaspersky Embedded Systems Security вместе с единственным указанным правилом. Будет разрешен запуск только тех программ, которые имеют статус доверенных в KSN, или запускать которые разрешает указанное правило.

> При использовании этого сценария рекомендуется задать правило, разрешающее запуск программ по цифровому сертификату.

Все остальные программы будут блокироваться в соответствии с принципом запрета по умолчанию. Применение KSN при отсутствии правил позволяет защитить устройство от программ, которые по данным KSN представляют угрозу.

Применение заключений KSN совместно с правилами контроля запуска программ

При использовании заключений KSN совместно с правилами контроля запуска программ применяются следующие условия:

- Kaspersky Embedded Systems Security всегда блокирует запуск программы, если она подпадает под действие хотя бы одного запрещающего правила. Если такая программа признана доверенной службами KSN, это заключение имеет меньший приоритет и не учитывается; программа все равно будет заблокирована. Это позволит расширить список заблокированных программ.

- Kaspersky Embedded Systems Security всегда блокирует запуск программы, если установлен запрет запуска программ, недоверенных в KSN, и данная программа признана недоверенной службами KSN. Если для этой программы задано разрешающее правило, оно имеет меньший приоритет и не учитывается; программа все равно будет заблокирована. Это позволяет защитить устройство от программ, которые по данным KSN представляют угрозу, но не были учтены при первоначальной настройке правил.

О формировании правил контроля запуска программ

Вы можете создать списки правил контроля запуска программ с помощью задач и политик Kaspersky Security Center одновременно для всех защищаемых устройств и групп защищаемых устройств в сети организации. Рекомендуется использовать перечисленные сценарии, если в сети организации нет эталонной машины и вы не можете сформировать список разрешающих правил на основе программ, установленным на такой эталонной машине.

Можно запустить задачу Формирование правил контроля запуска программ локально с помощью Консоли программы для создания списка правил на основе программ, запущенных на отдельном защищаемом устройстве.

По умолчанию компонент Контроль запуска программ устанавливается с двумя разрешающими правилами:

- Разрешающее правило для скриптов и пакетов установщика Windows с сертификатом, доверенным в операционной системе.
- Разрешающее правило для исполняемых файлов с сертификатом, доверенным в операционной системе.

Вы можете создавать списки правил контроля запуска программ на стороне Kaspersky Security Center двумя способами:

- С помощью групповой задачи Формирование правил контроля запуска программ.

  В рамках этого сценария групповая задача формирует собственный список правил контроля запуска программ для каждого защищаемого устройства в сети и сохраняет эти списки в XML-файл в указанной папке общего доступа. XML-файл, созданный задачей Формирование правил контроля запуска программ, содержит разрешающие правила, указанные при настройке параметров задачи, до ее запуска. Для программ, запуск которых не разрешен в параметрах указанной задачи, не будет создано ни одного правила. Запуск таких программ будет заблокирован по умолчанию. Затем вы можете вручную импортировать сформированные списки правил в задачу Контроль запуска программ для политики Kaspersky Security Center.

  Вы можете настроить автоматический импорт сформированных правил в список правил задачи Контроль запуска программ.

  Рекомендуется использовать этот сценарий, если требуется быстро сформировать списки правил контроля запуска программ. Запуск задачи Формирование правил контроля запуска программ по расписанию рекомендуется настраивать, только если область применения разрешающих правил включает папки, содержащие заведомо безопасные файлы.

  Перед запуском задачи Контроль запуска программ в сети убедитесь, что для всех защищаемых устройств настроен доступ к папке общего доступа. Если применение папки общего доступа не предусмотрено политикой организации, рекомендуется запустить задачу Формирование правил контроля запуска программ на защищаемом устройстве в тестовой группе защищаемых устройств или на эталонной машине.

- На основе отчета о событиях в работе задачи Контроль запуска программ в режиме **Только статистика**, сформированного в Kaspersky Security Center.

  В рамках этого сценария Kaspersky Embedded Systems Security не блокирует запуск программ. Когда задача Контроль запуска программ работает в режиме **Только статистика**, все разрешенные и запрещенные запуски программ на всех защищаемых устройствах сети регистрируются на закладке **События** в рабочей области узла Сервера администрирования в Kaspersky Security Center. С помощью отчетов в Kaspersky Security Center формируется единый список событий о заблокированных запусках программ.

  Вам нужно настроить период выполнения задачи так, чтобы за указанный промежуток времени выполнились все возможные сценарии работы защищаемых устройств и групп защищаемых устройств и хотя бы одна перезагрузка. После завершения выполнения задачи можно импортировать данные о запусках программ из сохраненного отчета о событиях Kaspersky Security Center (файла в формате TXT) и сформировать на основе этих данных разрешающие правила контроля запуска таких программ.

  Рекомендуется использовать этот сценарий, если в сети организации имеется большое количество защищаемых устройств разных типов с различным набором установленных программ.

- На основе событий блокировки запуска программ, полученных через Kaspersky Security Center, без создания и импорта конфигурационного файла.

  Чтобы воспользоваться данной возможностью, задача Контроль запуска программ на защищаемом устройстве должна находиться под управлением активной политики Kaspersky Security Center. При этом все события на защищаемом устройстве передаются на Сервер администрирования.

Рекомендуется обновить список правил при изменении состава программ, установленных на управляемых устройствах в сети (например, при установке обновлений или переустановке операционной системы). Рекомендуется сформировать обновленный список правил, запустив задачу Формирование правил контроля запуска программ или задачу Контроль запуска программ в режиме **Только статистика** на защищаемых устройствах тестовой группы администрирования. Тестовая группа администрирования включает защищаемые устройства, необходимые для тестового запуска новых программ перед их установкой на остальные защищаемые устройства сети.

XML-файлы, содержащие списки разрешающих правил, создаются на основе анализа задач, запускаемых на защищаемом устройстве. Чтобы при формировании списка правил учесть все используемые в сети программы, рекомендуется запускать задачи Формирование правил контроля запуска программ и Контроль запуска программ в режиме **Только статистика** на эталонной машине.

Перед формированием разрешающих правил на основе программ, запущенных на эталонной машине организации, убедитесь, что эталонная машина защищена и на ней нет вредоносных программ.

Перед добавлением разрешающих правил выберите один из доступных режимов применения правил. В списке правил политики Kaspersky Security Center отображаются только правила, заданные в этой политике, вне зависимости от режима применения правил. Список локальных правил включает все применимые правила: локальные и добавленные через политику.

Параметры по умолчанию для задачи Контроль запуска программ

По умолчанию задача Контроль запуска программ имеет параметры, описанные в таблице ниже. Вы можете изменять значения этих параметров.

Параметры по умолчанию для задачи Контроль запуска программ

Параметр	Значение по умолчанию	Описание
Режим работы	**Только статистика** Задача регистрирует события, соответствующие попыткам запуска программ, запрещенным или разрешенным на основе набора правил. Фактическая блокировка запуска программ не выполняется.	Вы можете выбрать режим **Активный** после того, как будет сформирован окончательный список правил.
Обрабатывать повторные запуски контролируемых программ по схеме обработки первого запуска	Применяется.	Можно повторять действия, выполненные с файлом при первом запуске, при всех последующих запусках.
Запрещать запуск командных	Не применяется.	Вы можете запрещать запуск командных интерпретаторов без исполняемых

интерпретаторов без команды к исполнению		команд.
Правила	**Заменить правилами политики локальные правила**	Вы можете выбрать режим совместного применения правил, заданных в политике, и правил на защищаемом устройстве.
Область применения правил	Задача контролирует запуск исполняемых файлов, скриптов и MSI-пакетов. Кроме того, она контролирует загрузку DLL-модулей.	Вы можете указывать типы файлов, запуск которых будет контролироваться правилами.
Использование KSN	Данные KSN о репутации программы не используются.	Вы можете использовать данные о репутации программ в KSN при работе задачи Контроль запуска программ.
Автоматически разрешать распространение с помощью указанных программ и пакетов установки	Не применяется.	Вы можете разрешать распространение программного обеспечения с помощью указанных в настройках пакетов установки и программ. По умолчанию распространение программ разрешено только с помощью служб установщика Windows.
Всегда разрешать распространение программ с помощью установщика Windows	Применяется. Можно изменить, только если включен параметр **Автоматически разрешать распространение с помощью указанных программ и пакетов установки**.	Вы можете разрешить установку или обновление любого программного обеспечения, если операции выполняются с помощью установщика Windows.
Всегда разрешать распространение программ через SCCM с помощью фоновой интеллектуальной службы передачи	Не применяется. Можно изменить, только если включен параметр **Автоматически разрешать распространение с помощью указанных программ и пакетов установки**.	Можно включить или выключить автоматическое распространение программного обеспечения с помощью решения System Center Configuration Manager.
Параметры запуска задачи	Время первого запуска не задано.	Задача Контроль запуска программ не запускается автоматически сразу после Kaspersky Embedded Systems Security. Вы можете запустить задачу вручную или настроить запуск задачи по расписанию.

Заданные по умолчанию параметры задачи Формирование правил контроля запуска программ

Параметр	Значение по умолчанию	Описание
Префикс для названий разрешающих правил	Совпадает с именем защищаемого устройства, на котором установлена программа Kaspersky Embedded Systems Security.	Вы можете изменить префикс для названий разрешающих правил.
Область применения разрешающих правил	Под область применения разрешающих правил по умолчанию подпадают следующие категории файлов: • файлы с расширением EXE, расположенные в папках	Вы можете изменить область защиты, добавляя или удаляя пути к папкам и указывая типы файлов, запуск которых будет разрешен автоматически сформированными правилами. Также при создании разрешающих правил вы можете не учитывать запущенные программы.

	C:\Windows, C:\Program Files (x86) и C:\Program Files; • пакеты MSI, расположенные в папке C:\Windows; • скрипты, расположенные в папке C:\Windows. Также задача создает правила для всех уже запущенных программ независимо от их расположения и формата.	
Критерии формирования разрешающих правил	Используется заголовок и отпечаток цифрового сертификата; правила формируются для всех пользователей и групп пользователей.	Вы можете использовать хеш SHA256 при формировании разрешающих правил. Вы можете выбрать пользователя и группу пользователей, для которых необходимо автоматически формировать разрешающие правила.
Действия по завершении задачи	Разрешающие правила добавляются в список правил контроля запуска программ; новые правила объединяются с существующими правилами; дублирующиеся правила удаляются.	Вы можете добавлять правила к уже существующим правилам без объединения и без удаления дублирующихся правил или заменять существующие правила новыми разрешающими правилами, а также настраивать параметры экспорта разрешающих правил в файл.
Параметры запуска задачи с правами	Задача запускается с правами системной учетной записи.	Вы можете разрешить запуск задачи Формирование правил контроля запуска программ с правами системной учетной записи или с правами указанного пользователя.
Расписание запуска задачи	Время первого запуска не задано.	Задача Формирование правил контроля запуска программ не запускается автоматически при запуске Kaspersky Embedded Systems Security. Вы можете запустить задачу вручную или настроить запуск задачи по расписанию.

Управление контролем запуска программ с помощью Плагина управления

В этом разделе описана навигация в интерфейсе Плагина управления и настройка параметров задачи для защищаемых устройств в сети.

Навигация

В этом разделе описан переход к требуемым параметрам задачи с помощью интерфейса.

Переход к параметрам политики для задачи Контроль запуска программ

Чтобы перейти к параметрам задачи Контроль запуска программ в политике Kaspersky Security Center, выполните следующие действия:

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой вы хотите настроить задачу.
3. Выберите закладку **Политики**.
4. Откройте окно свойств политики двойным щелчком мыши на имени политики, которую вы хотите настроить.
5. В открывшемся окне **Свойства: <Имя политики>** перейдите в раздел **Контроль активности на серверах**.
6. Нажмите на кнопку **Настройка** в подразделе **Контроль запуска программ**.

   Откроется окно **Контроль запуска программ**.

Настройте политику в соответствии с вашими требованиями.

Переход к списку правил контроля запуска программ

Чтобы перейти к списку правил контроля запуска программ в Kaspersky Security Center, выполните следующие действия:

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой вы хотите настроить задачу.
3. Выберите закладку **Политики**.
4. Откройте окно свойств политики двойным щелчком мыши на имени политики, которую вы хотите настроить.
5. В открывшемся окне **Свойства: <Имя политики>** перейдите в раздел **Контроль активности на серверах**.
6. Нажмите на кнопку **Настройка** в подразделе **Контроль запуска программ**.

   Откроется окно **Контроль запуска программ**.
7. На закладке **Общие** нажмите на кнопку **Список правил**.

   Откроется окно **Правила контроля запуска программ**.

Настройте список правил в соответствии с вашими требованиями.

Переход к мастеру создания задачи Формирование правил контроля запуска программ и ее свойствам

Чтобы создать задачу Формирование правил контроля запуска программ, выполните следующие действия:

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой вы хотите настроить задачу.
3. Выберите закладку **Задачи**.
4. Нажмите на кнопку **Создать задачу**.

   Откроется окно **Мастер создания задачи**.
5. Выберите задачу **Формирование правил контроля запуска программ**.
6. Нажмите на кнопку **Далее**.

   Откроется окно **Настройка**.

Чтобы настроить задачу Формирование правил контроля запуска программ, выполните следующие действия:

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой вы хотите настроить задачу.
3. Выберите закладку **Задачи**.
4. Выберите название задачи в списке задач Kaspersky Security Center двойным щелчком мыши.

   Откроется окно **Свойства: Формирование правил контроля запуска программ**.

Дополнительную информацию о настройке задачи см. в разделе Настройка задачи Формирование правил контроля запуска программ.

Настройка параметров задачи Контроль запуска программ

Чтобы настроить общие параметры задачи Контроль запуска программ, выполните следующие действия:

1. Откройте окно **Контроль запуска программ**.
2. На закладке **Общие** в разделе **Режим работы** настройте следующие параметры:
   - В раскрывающемся списке **Режим работы** выберите режим работы задачи.
   - Снимите или установите флажок **Обрабатывать повторные запуски контролируемых программ по схеме обработки первого запуска**.
   - Снимите или установите флажок **Запрещать запуск командных интерпретаторов без команды к исполнению**.
3. В блоке **Правила** настройте параметры применения правил:
   a. Нажмите на кнопку **Список правил**, чтобы добавить разрешающие правила в задачу Контроль запуска программ.

Kaspersky Embedded Systems Security не распознает путь, включающий наклонную черту ("/"). Используйте обратную наклонную черту ("\"), чтобы правильно ввести путь.

b. Выберите режим применения правил:

- **Заменить правилами политики локальные правила**

  Программа применяет список правил, заданных в политике, для централизованного контроля запуска программ на группе защищаемых устройств. Формирование, редактирование и применение локальных списков правил недоступно.

- **Добавить правила политики к локальным правилам**

  Программа применяет список правил, заданный в политике, совместно с локальными списками правил. Вы можете редактировать локальные списки правил с помощью задач автоматического формирования правил контроля запуска программ.

По умолчанию Kaspersky Embedded Systems Security применяет два стандартных правила, которые разрешают запуск скриптов, MSI-пакетов и исполняемых файлов, если эти объекты подписаны доверенной цифровой подписью.

4. В разделе **Область применения правил** укажите следующие параметры:

- **Использовать правила для исполняемых файлов**
- **Контролировать загрузку DLL-модулей**

  Контроль загрузки DLL-модулей может влиять на производительность операционной системы.

- **Использовать правила для скриптов и пакетов MSI**

5. В блоке параметров **Использование KSN** настройте следующие параметры запуска программ:

- **Запрещать запуск программ, недоверенных в KSN**
- **Разрешать запуск программ, доверенных в KSN**
- Пользователи и / или группы пользователей, которым разрешен запуск доверенных в KSN программ

6. На закладке **Контроль пакетов установки** настройте параметры контроля пакетов установки.

7. На закладке **Управление задачей** настройте параметры запуска задачи по расписанию.

8. В окне **Контроль запуска программ** нажмите на кнопку **OK**.

Kaspersky Embedded Systems Security немедленно применит новые значения параметров в выполняющейся задаче. Данные о дате и времени изменения параметров, а также значения параметров задачи до и после изменения будут сохранены в журнале системного аудита.

Настройка Контроля пакетов установки

Чтобы добавить доверенный пакет установки, выполните следующие действия:

1. Откройте окно **Контроль запуска программ**.
2. На закладке **Контроль пакетов установки** установите флажок **Автоматически разрешать распространение с помощью указанных программ и пакетов установки**.

   Вы можете установить флажок **Автоматически разрешать распространение с помощью указанных программ и пакетов установки**, если на закладке **Общие** в параметрах задачи **Контроль запуска программ** установлен флажок **Использовать правила для исполняемых файлов**.

3. При необходимости снимите флажок **Всегда разрешать распространение программ с помощью установщика Windows**.

   Флажок **Всегда разрешать распространение программ с помощью установщика Windows** рекомендуется снимать только в случае крайней необходимости. Выключение этой функции может привести к проблемам при обновлении файлов операционной системы, а также к блокированию запуска файлов, извлеченных из пакета установки.

4. Если требуется, установите флажок **Всегда разрешать распространение программ через SCCM с помощью фоновой интеллектуальной службы передачи**.

   Программа контролирует цикл распространения программного обеспечения на защищаемом устройстве: от доставки пакета до установки или обновления. Программа не контролирует процессы, если какой-то из этапов распространения был выполнен до установки программы на защищаемое устройство.

5. Чтобы отредактировать список доверенных пакетов установки, нажмите на кнопку **Изменить список пакетов** и в открывшемся окне выберите один из следующих способов:

   - **Добавить один вручную**.

     a. Нажмите на кнопку **Обзор**.

     b. Выберите исполняемый файл или пакет установки.

     Блок **Критерий доверенности** автоматически заполнится данными о выбранном файле.

     c. Снимите или установите флажок **Разрешать дальнейшее распространение программ, созданных от этого пакета установки**.

     d. Выберите один из двух доступных вариантов критериев доверенности, основываясь на которых файл или пакет установки будет считаться доверенным:

     - **Использовать цифровой сертификат**
     - **Использовать хеш SHA256**

   - **Добавить несколько по хешу**

     Вы можете выбрать неограниченное число исполняемых файлов и пакетов установки и добавить их в список одновременно. Kaspersky Embedded Systems Security учитывает хеш и разрешает запуск при обращении операционной системы к указанным файлам.

- **Изменить выбранный**

  Используйте этот вариант, чтобы выбрать другой исполняемый файл или пакет установки, а также изменить критерии доверенности.

- **Импортировать из текстового файла**

  В окне Открыть укажите конфигурационный файл со списком доверенных пакетов установки.

6. Если вы хотите удалить ранее добавленную программу или пакет установки из списка доверенных, нажмите на кнопку **Удалить пакет установки**. Запуск распакованных файлов будет разрешен.

   Чтобы запретить запуск извлеченных файлов, удалите программу с защищаемого устройства или создайте запрещающее правило в параметрах задачи Контроль запуска программ.

7. Нажмите на кнопку OK.

Настроенные параметры будут сохранены.

Настройка задачи Формирование правил контроля запуска программ

Чтобы настроить задачу Формирование правил контроля запуска программ, выполните следующие действия:

1. Откройте окно **Свойства: Формирование правил контроля запуска программ**.

2. В разделе **Уведомления** настройте параметры уведомлений о событиях задачи.

   Подробная информация о настройке параметров в этом разделе приведена в *Справке Kaspersky Security Center*.

3. В разделе **Настройка** можно настроить следующие параметры:

   - Укажите префикс для названий правил.
   - Выберите способ создания разрешающих правил:
     - **Создавать разрешающие правила на основе запущенных программ**
     - **Создавать разрешающие правила для программ из папок**

4. В разделе **Параметры** можно указать действия при формировании разрешающих правил контроля запуска программ:

   - **Использовать цифровой сертификат**
   - **Использовать заголовок и отпечаток цифрового сертификата**
   - **Если сертификат отсутствует, использовать**
     - **хеш SHA256** В качестве критерия срабатывания разрешающего правила контроля запуска программ устанавливается контрольная сумма файла, на основе которого формируется правило. В

дальнейшем программа будет разрешать запуск программ, запускаемых файлами с указанной контрольной суммой.

- **путь к файлу** В качестве критерия срабатывания разрешающего правила контроля запуска программ устанавливается путь к файлу, на основе которого формируется правило. В дальнейшем программа будет разрешать запуск программ теми файлами, которые находятся в папках, указанных в таблице **Создавать разрешающие правила для программ из папок** в разделе **Настройка**.

- **Использовать хеш SHA256**
- **Формировать правила для пользователя или группы пользователей**.

Вы можете настроить параметры для конфигурационных файлов со списком сформированных разрешающих правил контроля устройств и контроля запуска программ, которые Kaspersky Embedded Systems Security создает по завершении задач.

5. В разделе **Расписание** настройте параметры расписания задачи (вы можете настраивать расписание всех задач, кроме задачи Откат обновления баз программы).

6. В разделе **Учетная запись** укажите учетную запись, с правами которой будет выполняться задача.

7. Если требуется, в разделе **Исключения** из области действия задачи укажите объекты, которые хотите исключить из области действия задачи.

   Подробная информация о настройке параметров в этом разделе приведена в *Справке Kaspersky Security Center*.

8. В окне **Свойства: <Название задачи>** нажмите на кнопку **OK**.

   Настроенные параметры групповых задач будут сохранены.

Настройка правил контроля запуска программ в Kaspersky Security Center

В этом разделе описано формирование списка правил на основе различных критериев, а также создание разрешающих и запрещающих правил вручную с помощью задачи Контроль запуска программ.

Добавление правила контроля запуска программ

Чтобы добавить правило контроля запуска программ, выполните следующие действия:

1. Откройте окно **Правила контроля запуска программ**.

2. Нажмите на кнопку **Добавить**.

3. В контекстном меню кнопки выберите пункт **Добавить одно правило**.

   Откроется окно **Параметры правила**.

4. Укажите следующие параметры:

a. В поле **Название** введите название правила.

b. В раскрывающемся списке **Тип** выберите тип правила:

- **Разрешающее**, если вы хотите, чтобы правило разрешало запуск программ в соответствии с критериями, указанными в параметрах правила.
- **Запрещающее**, если вы хотите, чтобы правило блокировало запуск программ в соответствии с критериями, указанными в параметрах правила.

c. В раскрывающемся списке **Область применения** выберите тип файлов, запуск которых будет контролировать правило:

- **Исполняемые файлы**, если вы хотите, чтобы правило контролировало запуск исполняемых файлов.
- **Скрипты и пакеты MSI**, если вы хотите, чтобы правило контролировало запуск скриптов и пакетов MSI.

d. В поле **Пользователь или группа пользователей** укажите пользователей, которым будет разрешено или запрещено запускать программы в соответствии с типом правила. Для этого выполните следующие действия:

1. Нажмите на кнопку **Выбрать**.
2. Откроется стандартное окно Microsoft Windows Выбор пользователя или группы.
3. Задайте список пользователей и / групп пользователей.
4. Нажмите на кнопку OK.

e. Чтобы использовать значения критериев срабатывания правила, перечисленных в блоке **Критерий срабатывания правила**, из файла, выполните следующие действия:

1. Нажмите на кнопку **Задать критерий срабатывания правила из свойств файла**.

   Откроется стандартное окно Microsoft Windows Открыть.
2. Выберите файл.
3. Нажмите на кнопку Открыть.

   Значения критериев из файла отобразятся в полях блока **Критерий срабатывания правила**. По умолчанию будет выбран первый в списке критерий, данные для которого присутствуют в свойствах файла.

f. В блоке параметров **Критерий срабатывания правила** выберите один из следующих вариантов:

- **Цифровой сертификат**, если вы хотите, чтобы правило контролировало запуск программ с помощью файлов, подписанных цифровым сертификатом:
  - Установите флажок **Использовать заголовок**, если вы хотите, чтобы правило контролировало запуск файлов, подписанных цифровым сертификатом только с указанным заголовком.
  - Установите флажок **Использовать отпечаток**, если вы хотите, чтобы правило контролировало только запуск файлов, подписанных цифровым сертификатом с указанным отпечатком.
- **Хеш SHA256**, если вы хотите, чтобы правило контролировало запуск программ с помощью файлов, контрольная сумма которых соответствует указанной.

- **Путь к файлу**, если вы хотите, чтобы правило контролировало запуск программ из файлов, расположенных по указанному пути.

  Kaspersky Embedded Systems Security не распознает путь, включающий наклонную черту ("/"). Используйте обратную наклонную черту ("\"), чтобы правильно ввести путь.

g. Если вы хотите добавить исключения из правила, выполните следующие действия:

1. В разделе **Исключения из правила** нажмите на кнопку Добавить.

   Откроется окно **Исключение из правила**.

2. В поле **Название** введите название исключения.

3. Укажите параметры исключения файлов программ из правила контроля запуска программ. Вы можете заполнить поля параметров из свойств файла по кнопке **Задать исключение на основе свойств файла**.

   - Цифровой сертификат
   - **Использовать заголовок**
   - **Использовать отпечаток**
   - **Хеш SHA256**
   - **Путь к файлу**

4. Нажмите на кнопку **OK**.

5. Повторите пункты (i)-(iv) для добавления дополнительных исключений.

5. В окне **Параметры правила** нажмите на кнопку **OK**.

Созданное правило отобразится в списке в окне **Правила контроля запуска программ**.

Включение режима разрешения по умолчанию

Режим разрешения по умолчанию разрешает запуск всех программ, если они не запрещены правилами и не являются недоверенными согласно заключению KSN. Режим разрешения по умолчанию можно включить с помощью специальных разрешающих правил. Вы можете включить разрешение по умолчанию только для скриптов или для всех исполняемых файлов.

Чтобы добавить правило разрешения по умолчанию, выполните следующие действия:

1. Откройте окно Правила контроля запуска программ.

2. Нажмите на кнопку **Добавить** и в открывшемся контекстном меню выберите пункт **Добавить одно правило**.

   Откроется окно **Параметры правила**.

3. В поле **Название** введите название правила.

4. В раскрывающемся списке **Тип** выберите элемент **Разрешающее**.

5. В раскрывающемся списке **Область применения** выберите тип файлов, запуск которых будет контролировать правило:

   - **Исполняемые файлы**, если вы хотите, чтобы правило контролировало запуск исполняемых файлов;
   - **Скрипты и пакеты MSI**, если вы хотите, чтобы правило контролировало запуск скриптов и пакетов MSI.

6. В блоке параметров **Критерий срабатывания правила** выберите вариант **Путь к файлу**.
7. Введите следующую маску: `?:\`
8. В окне **Параметры правила** нажмите на кнопку **ОК**.

Kaspersky Embedded Systems Security применяет режим разрешения по умолчанию.

Создание разрешающих правил на основе событий Kaspersky Security Center

Чтобы сформировать разрешающие правила контроля запуска программ для программ из событий Kaspersky Security Center, выполните следующие действия:

1. Откройте окно Правила контроля запуска программ.
2. Нажмите на кнопку **Добавить** и в контекстном меню кнопки выберите пункт **Создать разрешающие правила программ из событий Kaspersky Security Center**.
3. Выберите принцип добавления правил к списку уже созданных правил контроля запуска программ:

   - **Добавить правила к существующим**, если требуется, чтобы импортируемые правила были добавлены в список существующих правил. Правила с одинаковыми параметрами дублируют друг друга.
   - **Заменить существующие правила**, если вы хотите, чтобы импортируемые правила заменили существующие правила.
   - **Объединить правила с существующими**, если вы хотите, чтобы импортируемые правила были добавлены в список существующих правил. Правила с дублирующими параметрами не добавляются; если хотя бы один параметр правила уникален, правило добавляется.

   Откроется окно **Создать правила контроля запуска программ**.

4. Настройте следующие параметры запроса:

   - **Адрес Сервера администрирования**
   - **Порт**
   - **Пользователь**
   - **Пароль**

5. Выберите типы событий, которые должны стать основой для задачи формирования правил:

   - **Только статистика: запуск программы запрещен**.

- **Запуск программы запрещен**.

6. Выберите период из раскрывающегося списка **Учитывать события, сформированные в течение периода**.

7. Снимите или установить флажок **Приоритизировать использование контрольной суммы при создании правил**.

   Если флажок установлен, Kaspersky Embedded Systems Security использует контрольную сумму (хеш) файла для формирования правила, когда доступны и контрольная сумма, и сертификат файла.

   Если флажок снят, Kaspersky Embedded Systems Security использует цифровой сертификат файла для формирования правила, когда доступны и контрольная сумма, и сертификат файла.

8. Нажмите на кнопку **Создать правила**.

9. Нажмите на кнопку **Сохранить** в окне **Правила контроля запуска программ**.

   Список правил в задаче Контроль запуска программ будет дополнен новыми правилами, сформированными на основе системных данных защищаемого устройства, на котором установлена Консоль администрирования Kaspersky Security Center.

   Если список правил контроля запуска программ уже задан в политике, Kaspersky Embedded Systems Security добавит выбранные правила из событий блокирования к уже заданным правилам. Правила с повторяющимся хешем не добавляются, поскольку все правила в списке должны быть уникальными.

Импорт правил из отчета Kaspersky Security Center о заблокированных программах

Вы можете импортировать данные о заблокированных запусках программ из отчета, сформированного в Kaspersky Security Center по результатам выполнения задачи Контроль запуска программ в режиме **Только статистика**, и применить эти данные для формирования списка разрешающих правил запуска программ в настраиваемой политике.

При формировании отчета о событиях, возникающих в ходе выполнения задачи Контроль запуска программ, вы можете отслеживать программы, запуск которых был заблокирован.

При импорте из отчета данных о заблокированных программах в свойства политики убедитесь, что применяемый список содержит только те программы, запуск которых вы хотите разрешить.

Чтобы задать разрешающие правила контроля запуска программ для группы защищаемых устройств на основе отчета о заблокированных программах из Kaspersky Security Center, выполните следующие действия:

1. Откройте окно **Контроль запуска программ**.

2. В блоке **Режим работы** выберите режим **Только статистика**.

3. В свойствах политики в разделе **Уведомления о событиях** убедитесь, что:

   - Для событий с уровнем важности **Критический** срок хранения событий **Запуск программы запрещен** в журнале выполнения задачи превышает запланированный период выполнения задачи в режиме

Только статистика (значение по умолчанию – 30 дней).

- Для событий с уровнем важности **Предупреждение** срок хранения событий **Только статистика: запуск программы запрещен** в журнале выполнения задачи превышает запланированный период выполнения задачи в режиме **Только статистика** (значение по умолчанию – 30 дней).

  По истечении срока хранения событий информация о зарегистрированных событиях будет удалена и не попадет в файл отчета. Перед запуском задачи Контроль запуска программ в режиме **Только статистика** убедитесь, что время выполнения задачи не превышает установленный срок хранения указанных событий.

4. По завершении задачи выполните экспорт зарегистрированных событий в файл формата TXT:

   a. В Kaspersky Security Center в рабочей области узла **Сервер администрирования** выберите закладку **События**.

   b. Нажмите на кнопку **Создать выборку**, чтобы создать выборку событий по критерию Заблокировано и просмотреть, запуск каких программ будет заблокирован задачей Контроль запуска программ.

   c. В панели результатов созданной выборки перейдите по ссылке **Экспортировать события в файл**, чтобы сохранить отчет о заблокированных запусках программ в файл формата TXT.

   Перед импортом и применением сформированного отчета в политике убедитесь, что отчет содержит данные только о тех программах, запуск которых требуется разрешить.

5. Импортируйте данные о заблокированных запусках программ в задачу контроля запуска программ. Для этого в свойствах политики в параметрах задачи Контроль запуска программ выполните следующие действия:

   a. На закладке **Общие** нажмите на кнопку **Список правил**.

   Откроется окно **Правила контроля запуска программ**.

   b. Нажмите на кнопку **Добавить** и в контекстном меню кнопки выберите пункт **Импортировать данные о заблокированных программах из отчета Kaspersky Security Center**.

   c. Выберите принцип добавления правил из списка, созданного на основе отчета Kaspersky Security Center, к списку настроенных ранее правил контроля запуска программ:

      - **Добавить правила к существующим**, если требуется, чтобы импортируемые правила были добавлены в список существующих правил. Правила с одинаковыми параметрами дублируют друг друга.

      - **Заменить существующие правила**, если вы хотите, чтобы импортируемые правила заменили существующие правила.

      - **Объединить правила с существующими**, если вы хотите, чтобы импортируемые правила были добавлены в список существующих правил. Правила с дублирующими параметрами не добавляются; если хотя бы один параметр правила уникален, правило добавляется.

   d. В открывшемся стандартном окне Microsoft Windows выберите файл формата TXT, в который были экспортированы события из отчета о заблокированных запусках программ.

   e. Нажмите на кнопку **Сохранить** в окне **Правила контроля запуска программ**.

Правила, созданные на основе отчета Kaspersky Security Center о заблокированных программах, будут добавлены к списку правил контроля запуска программ.

Импорт правил контроля запуска программ из XML-файла

Вы можете импортировать отчеты, сформированные по результатам выполнения групповой задачи Формирование правил контроля запуска программ, и применить их в качестве списка разрешающих правил в настраиваемой политике.

По завершении групповой задачи формирования правил контроля запуска программ выполняется экспорт созданных разрешающих правил в XML-файлы в указанную папку общего доступа. Каждый файл со списком правил создается на основе анализа исполняемых файлов и запущенных программ на каждом отдельном защищаемом устройстве в сети организации. Списки содержат разрешающие правила для файлов и программ, тип которых соответствует параметрам, указанным в групповой задаче формирования правил контроля запуска программ.

Чтобы задать разрешающие правила контроля запуска программ для группы защищаемых устройств на основе автоматически сформированного списка разрешающих правил, выполните следующие действия:

1. На закладке **Задачи** в панели результатов настраиваемой группы защищаемых устройств создайте групповую задачу Формирование правил контроля запуска программ или выберите уже созданную задачу.

2. В свойствах созданной групповой задачи Формирование правил контроля запуска программ или в мастере создания задачи настройте следующие параметры:

   - В разделе **Уведомление** настройте параметры сохранения отчета выполнения задачи.

     Подробная информация о настройке параметров в этом разделе приведена в *Справке Kaspersky Security Center*.

   - В разделе **Настройка** укажите типы программ, запуск которых будет разрешен созданными правилами. Можно изменить набор папок, содержащих разрешенные для запуска программы: исключать из области действия задачи папки, указанные по умолчанию, и добавлять новые папки вручную.

   - В разделе **Параметры** укажите действия, выполняемые задачей во время работы и после завершения. Укажите критерий формирования правил и имя файла, в который будут экспортированы эти правила.

   - В разделе **Расписание** настройте параметры запуска задачи по расписанию.

   - В разделе **Учетная запись** укажите учетную запись пользователя, с правами которой будет выполняться задача.

   - В блоке **Исключения из области действия задачи** задайте группы защищаемых устройств, которые вы хотите исключить из области действия задачи.

     Kaspersky Embedded Systems Security не будет создавать разрешающие правила по программам, запускаемым на исключенных защищаемых устройствах.

3. На закладке **Задачи** панели результатов настраиваемой группы защищаемых устройств в списке групповых задач выберите созданную задачу Формирование правил контроля запуска программ и нажмите на кнопку **Запустить** для запуска задачи.

После завершения задачи, автоматически сформированные списки разрешающих правил будут сохранены в XML-файлы в папке общего доступа.

Перед запуском задачи Контроль запуска программ в сети убедитесь, что для всех защищаемых устройств настроен доступ к папке общего доступа. Если применение папки общего доступа не предусмотрено политикой организации, рекомендуется запустить задачу Формирование правил контроля запуска программ на защищаемом устройстве в тестовой группе защищаемых устройств или на эталонной машине.

4. Чтобы добавить сформированные списки разрешающих правил в задачу Контроль запуска программ, выполните следующие действия:

   a. Откройте окно **Правила контроля запуска программ**.

   b. Нажмите на кнопку **Добавить** и в открывшемся списке выберите пункт **Импортировать правила из файла формата XML**.

   c. Выберите принцип добавления автоматически сформированных разрешающих правил к списку уже заданных правил контроля запуска программ:

      - **Добавить правила к существующим**, если требуется, чтобы импортируемые правила были добавлены в список существующих правил. Правила с одинаковыми параметрами дублируют друг друга.

      - **Заменить существующие правила**, если вы хотите, чтобы импортируемые правила заменили существующие правила.

      - **Объединить правила с существующими**, если вы хотите, чтобы импортируемые правила были добавлены в список существующих правил. Правила с дублирующими параметрами не добавляются; если хотя бы один параметр правила уникален, правило добавляется.

   d. В открывшемся стандартном окне Microsoft Windows выберите XML-файлы, созданные по завершении групповой задачи Формирование правил контроля запуска программ.

   e. Нажмите на кнопку **Сохранить** в окне **Правила контроля запуска программ**.

5. Если вы хотите применять созданные правила для контроля запуска программ, в политике в свойствах задачи Контроль запуска программ выберите режим **Активный**.

Разрешающие правила, автоматически сформированные на основе запусков задач на каждом отдельном защищаемом устройстве, будут применены на всех защищаемых устройствах в сети, на которые распространяется настраиваемая политика. Для этих защищаемых устройств программа разрешит запуск только тех программ, для которых созданы разрешающие правила.

Проверка запуска программ

Перед применением заданных правил контроля запуска программ вы можете проверить любую программу, чтобы определить, какие правила контроля запуска программ срабатывают для выбранной программы.

По умолчанию Kaspersky Embedded Systems Security блокирует программы, запуск которых не разрешен хотя бы одним правилом. Чтобы избежать блокировки запуска важных программ, необходимо создать для них разрешающие правила.

Если запуск программы контролируется несколькими правилами разных типов, запрещающие правила имеют больший приоритет: запуск программы блокируется, если она подпадает под действие хотя бы одного запрещающего правила.

Чтобы проверить правила контроля запуска программ, выполните следующие действия:

1. Откройте окно **Правила контроля запуска программ**.
2. В открывшемся окне нажмите на кнопку **Показать правила для файла**.

   Откроется стандартное окно Microsoft Windows.
3. Выберите файл, контроль запуска которого хотите протестировать.

В строке поиска отобразится путь к указанному файлу. В списке правил отобразятся все правила, которые сработают при запуске указанного файла.

Создание задачи Формирование правил контроля запуска программ

Чтобы создать задачу Формирование правил контроля запуска программ и настроить ее параметры, выполните следующие действия:

1. Откройте окно **Настройка** в мастере создания задачи.
2. Настройте следующие параметры:
   - Укажите Префикс для названий правил.
   - Настройте область применения разрешающих правил.
3. Нажмите на кнопку Далее.
4. Укажите действия, которые должна выполнять программа Kaspersky Embedded Systems Security:
   - при формировании разрешающих правил;
   - по завершении задачи.
5. В окне **Расписание** укажите параметры запуска задачи по расписанию.
6. Нажмите на кнопку Далее.
7. В окне Выбор учетной записи для запуска задачи укажите требуемую учетную запись.
8. Нажмите на кнопку Далее.
9. Укажите название задачи.
10. Нажмите на кнопку Далее.

Название задачи не должно быть длиннее 100 символов и не должно содержать следующие символы: " * < > & \ : |

Откроется окно Завершение создания задачи.

11. По завершении работы мастера можно запустить задачу, установив флажок Запустить задачу после завершения работы мастера.

12. Нажмите на кнопку Завершить, чтобы завершить создание задачи.

Чтобы настроить существующее правило в Kaspersky Security Center,

откройте окно **Свойства:** **Формирование правил контроля запуска программ** и настройте параметры, как описано выше.

Данные о дате и времени изменения параметров, а также значения параметров задачи до и после изменения будут сохранены в журнале системного аудита.

Ограничение области действия задачи

Чтобы ограничить область действия задачи Формирование правил контроля запуска программ, выполните следующие действия:

1. Откройте окно **Свойства: Формирование правил контроля запуска программ**.

2. Выберите способ создания разрешающих правил:

   - **Создавать разрешающие правила на основе запущенных программ**
   - **Создавать разрешающие правила для программ из папок**

3. Нажмите на кнопку OK.

Настроенные параметры будут сохранены.

Действия при автоматическом формировании правил

Чтобы настроить действия Kaspersky Embedded Systems Security во время выполнения задачи Формирование правил контроля запуска программ, выполните следующие действия:

1. Откройте окно **Свойства: Формирование правил контроля запуска программ**.

2. Выберите закладку **Параметры**.

3. В блоке **При формировании разрешающих правил** настройте следующие параметры:

   - **Использовать цифровой сертификат**
   - **Использовать заголовок и отпечаток цифрового сертификата**
   - **Если сертификат отсутствует, использовать**
     - **хеш SHA256** В качестве критерия срабатывания разрешающего правила контроля запуска программ устанавливается контрольная сумма файла, на основе которого формируется правило. В дальнейшем программа будет разрешать запуск программ, запускаемых файлами с указанной контрольной суммой.

- **путь к файлу** В качестве критерия срабатывания разрешающего правила контроля запуска программ устанавливается путь к файлу, на основе которого формируется правило. В дальнейшем программа будет разрешать запуск программ теми файлами, которые находятся в папках, указанных в таблице **Создавать разрешающие правила для программ из папок** в разделе **Настройка**.

- **Использовать хеш SHA256**
- **Формировать правила для пользователя или группы пользователей**.

4. Нажмите на кнопку **ОК**.

Настроенные параметры будут сохранены.

Действия по завершении автоматического формирования правил

Чтобы настроить действия Kaspersky Embedded Systems Security по завершении выполнения задачи Формирование правил контроля запуска программ, выполните следующие действия:

1. Откройте окно **Свойства: Формирование правил контроля запуска программ**.
2. Выберите закладку **Параметры**.
3. В блоке **По завершении задачи** настройте следующие параметры:
   - **Добавлять разрешающие правила в список правил контроля запуска программ**
   - **Принцип добавления**
   - **Экспортировать разрешающие правила в файл**
   - **Добавлять информацию о компьютере в имя файла**
4. Нажмите на кнопку OK.

Настроенные параметры будут сохранены.

Управление контролем запуска программ с помощью Консоли программы

В этом разделе описана навигация в интерфейсе Консоли программы и настройка параметров задачи на защищаемом устройстве.

Навигация

В этом разделе описан переход к требуемым параметрам задачи с помощью интерфейса.

Переход к параметрам задачи Контроль запуска программ

Чтобы перейти к общим параметрам задачи Контроль запуска программ в Консоли программы, выполните следующие действия:

1. В дереве Консоли программы разверните узел **Контроль компьютера**.
2. Выберите вложенный узел **Контроль запуска программ**.
3. В панели результатов узла **Контроль запуска программ** перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи**.

Переход к окну с правилами контроля запуска программ

Чтобы перейти к списку правил контроля запуска программ в Консоли программы, выполните следующие действия:

1. В дереве Консоли программы разверните узел **Контроль компьютера**.
2. Выберите вложенный узел **Контроль запуска программ**.
3. В панели результатов узла **Контроль запуска программ** перейдите по ссылке **Правила контроля запуска программ**.

   Откроется окно **Правила контроля запуска программ**.
4. Настройте список правил в соответствии с вашими требованиями.

Переход к параметрам задачи Формирование правил контроля запуска программ

Чтобы настроить задачу Формирование правил контроля запуска программ, выполните следующие действия:

1. В дереве Консоли программы разверните узел **Автоматическое формирование правил**.
2. Выберите вложенный узел **Формирование правил контроля запуска программ**.
3. В панели результатов узла **Формирование правил контроля запуска программ** перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи**.
4. Настройте задачу в соответствии с вашими требованиями.

Настройка параметров задачи Контроль запуска программ

Чтобы настроить общие параметры задачи Контроль запуска программ, выполните следующие действия:

1. Откройте окно **Параметры задачи**.

2. Настройте следующие параметры задачи:

   - На закладке **Общие**:
     - Режим работы задачи Контроль запуска программ.
     - Область применения правил в задаче.
     - Использование KSN.
   - Параметры контроля пакетов установки на закладке **Контроль пакетов установки**.
   - Расписание запуска задачи на закладках **Расписание** и **Дополнительно**.

3. В окне **Параметры задачи** нажмите на кнопку **OK**.

   Изменения параметров задачи будут сохранены.

Kaspersky Embedded Systems Security немедленно применит новые значения параметров в выполняющейся задаче. Данные о дате и времени изменения параметров, а также значения параметров задачи до и после изменения будут сохранены в журнале системного аудита.

Выбор режима работы задачи Контроль запуска программ

Чтобы настроить режим работы задачи Контроль запуска программ, выполните следующие действия:

1. Откройте окно **Параметры задачи**.
2. На закладке **Общие** в раскрывающемся списке **Режим работы** выберите режим работы задачи.
3. Снимите или установите флажок **Обрабатывать повторные запуски контролируемых программ по схеме обработки первого запуска**.

   Kaspersky Embedded Systems Security заводит новый список событий в кеше при каждом изменении параметров задачи Контроль запуска программ. Таким образом, контроль запуска программ осуществляется в соответствии с актуальными параметрами безопасности.

4. Снимите или установите флажок **Запрещать запуск командных интерпретаторов без команды к исполнению**.
5. В окне **Параметры задачи** нажмите на кнопку **OK**.

   Настроенные параметры будут сохранены.

Все попытки запуска программ фиксируются в журнале выполнения задач.

Настройка области действия задачи Контроль запуска программ

Чтобы задать область действия задачи Контроль запуска программ, выполните следующие действия:

1. Откройте окно **Параметры задачи**.
2. На закладке **Общие** в блоке **Область применения правил** задайте следующие параметры:
   - **Использовать правила для исполняемых файлов**
   - **Контролировать загрузку DLL-модулей**

     Контроль загрузки DLL-модулей может влиять на производительность операционной системы.

   - **Использовать правила для скриптов и пакетов MSI**
3. В окне **Параметры задачи** нажмите на кнопку **OK**.

Настроенные параметры будут сохранены.

Настройка использования KSN

Чтобы настроить использование служб KSN в задаче Контроль запуска программ, выполните следующие действия:

1. Откройте окно **Параметры задачи**.
2. На закладке **Общие** в блоке **Использование KSN** укажите параметры использования служб KSN:
   - Если требуется, установите флажок **Запрещать запуск программ, недоверенных в KSN**.
   - Если требуется, установите флажок **Разрешать запуск программ, доверенных в KSN**.
   - Если установлен флажок **Разрешать запуск программ, доверенных в KSN**, укажите пользователей и группы пользователей, которым разрешен запуск доверенных в KSN программ. Для этого выполните следующие действия:

     a. Нажмите на кнопку **Изменить**.

     Откроется стандартное окно Microsoft Windows **Выбор пользователей или групп**.

     b. Задайте список пользователей и / или групп пользователей.

     c. Нажмите на кнопку **OK**.
3. В окне **Параметры задачи** нажмите на кнопку **OK**.

Настроенные параметры будут сохранены.

Контроль пакетов установки

Чтобы добавить доверенный пакет установки, выполните следующие действия:

1. Откройте окно **Параметры задачи**.

2. На закладке **Контроль пакетов установки** установите флажок **Автоматически разрешать распространение с помощью указанных программ и пакетов установки**.

   Вы можете установить флажок **Автоматически разрешать распространение с помощью указанных программ и пакетов установки**, если на закладке **Общие** в параметрах задачи **Контроль запуска программ** установлен флажок **Использовать правила для исполняемых файлов**.

3. При необходимости снимите флажок **Всегда разрешать распространение программ с помощью установщика Windows**.

   Флажок **Всегда разрешать распространение программ с помощью установщика Windows** рекомендуется снимать только в случае крайней необходимости. Выключение этой функции может привести к проблемам при обновлении файлов операционной системы, а также к блокированию запуска файлов, извлеченных из пакета установки.

4. Если требуется, установите флажок **Всегда разрешать распространение программ через SCCM с помощью фоновой интеллектуальной службы передачи**.

   Программа контролирует цикл распространения программного обеспечения на защищаемом устройстве: от доставки пакета до установки или обновления. Программа не контролирует процессы, если какой-то из этапов распространения был выполнен до установки программы на защищаемое устройство.

5. Чтобы отредактировать список доверенных пакетов установки, нажмите на кнопку **Изменить список пакетов** и в открывшемся окне выберите один из следующих способов:

   - **Добавить один вручную**.

     a. Нажмите на кнопку **Обзор**.

     b. Выберите исполняемый файл или пакет установки.

     Блок **Критерий доверенности** автоматически заполнится данными о выбранном файле.

     c. Снимите или установите флажок **Разрешать дальнейшее распространение программ, созданных от этого пакета установки**.

     d. Выберите один из двух доступных вариантов критериев доверенности, основываясь на которых файл или пакет установки будет считаться доверенным:

     - **Использовать цифровой сертификат**
     - **Использовать хеш SHA256**

   - **Добавить несколько по хешу**

     Вы можете выбрать неограниченное число исполняемых файлов и пакетов установки и добавить их в список одновременно. Kaspersky Embedded Systems Security учитывает хеш и разрешает запуск при обращении операционной системы к указанным файлам.

   - **Изменить выбранный**

Используйте этот вариант, чтобы выбрать другой исполняемый файл или пакет установки, а также изменить критерии доверенности.

- **Импортировать из текстового файла**

  В окне **Открыть** укажите конфигурационный файл со списком доверенных пакетов установки.

6. Если вы хотите удалить ранее добавленную программу или пакет установки из списка доверенных, нажмите на кнопку **Удалить пакет установки**. Запуск распакованных файлов будет разрешен.

   Чтобы запретить запуск извлеченных файлов, удалите программу с защищаемого устройства или создайте запрещающее правило в параметрах задачи Контроль запуска программ.

7. Нажмите на кнопку **OK**.

Настроенные параметры будут сохранены.

Настройка правил контроля запуска программ

В этом разделе описано формирование, импорт и экспорт списка правил, а также создание разрешающих и запрещающих правил вручную с помощью задачи Контроль запуска программ.

Добавление правила контроля запуска программ

Чтобы добавить правило контроля запуска программ, выполните следующие действия:

1. Откройте окно **Правила контроля запуска программ**.
2. Нажмите на кнопку **Добавить**.
3. В контекстном меню кнопки выберите пункт **Добавить одно правило**.

   Откроется окно **Параметры правила**.

4. Укажите следующие параметры:

   a. В поле **Название** введите название правила.

   b. В раскрывающемся списке **Тип** выберите тип правила:

   - **Разрешающее**, если вы хотите, чтобы правило разрешало запуск программ в соответствии с критериями, указанными в параметрах правила.
   - **Запрещающее**, если вы хотите, чтобы правило блокировало запуск программ в соответствии с критериями, указанными в параметрах правила.

   c. В раскрывающемся списке **Область применения** выберите тип файлов, запуск которых будет контролировать правило:

   - **Исполняемые файлы**, если вы хотите, чтобы правило контролировало запуск исполняемых файлов.

- **Скрипты и пакеты MSI**, если вы хотите, чтобы правило контролировало запуск скриптов и пакетов MSI.

d. В поле **Пользователь или группа пользователей** укажите пользователей, которым будет разрешено или запрещено запускать программы в соответствии с типом правила. Для этого выполните следующие действия:

1. Нажмите на кнопку **Выбрать**.
2. Откроется стандартное окно Microsoft Windows **Выбор пользователя или групп**.
3. Задайте список пользователей и / или групп пользователей.
4. Нажмите на кнопку **OK**.

e. Чтобы использовать значения критериев срабатывания правила, перечисленных в блоке **Критерий срабатывания правила**, из файла, выполните следующие действия:

1. Нажмите на кнопку **Задать критерий срабатывания правила из свойств файла**.

   Откроется стандартное окно Microsoft Windows **Открыть**.
2. Выберите файл.
3. Нажмите на кнопку **Открыть**.

   Значения критериев из файла отобразятся в полях блока **Критерий срабатывания правила**. По умолчанию будет выбран первый в списке критерий, данные для которого присутствуют в свойствах файла.

f. В блоке параметров **Критерий срабатывания правила** выберите один из следующих вариантов:

- **Цифровой сертификат**, если вы хотите, чтобы правило контролировало запуск программ с помощью файлов, подписанных цифровым сертификатом:
  - Установите флажок **Использовать заголовок**, если вы хотите, чтобы правило контролировало запуск файлов, подписанных цифровым сертификатом только с указанным заголовком.
  - Установите флажок **Использовать отпечаток**, если вы хотите, чтобы правило контролировало только запуск файлов, подписанных цифровым сертификатом с указанным отпечатком.
- **Хеш SHA256**, если вы хотите, чтобы правило контролировало запуск программ с помощью файлов, контрольная сумма которых соответствует указанной.
- **Путь к файлу**, если вы хотите, чтобы правило контролировало запуск программ из файлов, расположенных по указанному пути.

  Kaspersky Embedded Systems Security не распознает путь, включающий наклонную черту ("/"). Используйте обратную наклонную черту ("\"), чтобы правильно ввести путь.

g. Если вы хотите добавить исключения из правила, выполните следующие действия:

1. В блоке **Исключения из правила** нажмите на кнопку **Добавить**.

   Откроется окно **Исключение из правила**.
2. В поле **Название** введите название исключения.

3. Укажите параметры исключения файлов программ из правила контроля запуска программ. Вы можете заполнить поля параметров из свойств файла по кнопке **Задать исключение на основе свойств файла**.

   - **Цифровой сертификат**
   - **Использовать заголовок**
   - **Использовать отпечаток**
   - **Хеш SHA256**
   - **Путь к файлу**

4. Нажмите на кнопку **OK**.

5. Повторите пункты (i)-(iv) для добавления дополнительных исключений.

5. В окне **Параметры правила** нажмите на кнопку **OK**.

Созданное правило отобразится в списке в окне **Правила контроля запуска программ**.

Включение режима разрешения по умолчанию

Режим разрешения по умолчанию разрешает запуск всех программ, если они не запрещены правилами и не являются недоверенными согласно заключению KSN. Режим разрешения по умолчанию можно включить с помощью специальных разрешающих правил. Вы можете включить разрешение по умолчанию только для скриптов или для всех исполняемых файлов.

Чтобы добавить правило разрешения по умолчанию, выполните следующие действия:

1. Откройте окно **Правила контроля запуска программ**.
2. Нажмите на кнопку **Добавить**.
3. В контекстном меню кнопки выберите пункт **Добавить одно правило**.

   Откроется окно **Параметры правила**.
4. В поле **Название** введите название правила.
5. В раскрывающемся списке **Тип** выберите элемент **Разрешающее**.
6. В раскрывающемся списке **Область применения** выберите тип файлов, запуск которых будет контролировать правило:

   - **Исполняемые файлы**, если вы хотите, чтобы правило контролировало запуск исполняемых файлов;
   - **Скрипты и пакеты MSI**, если вы хотите, чтобы правило контролировало запуск скриптов и пакетов MSI.
7. В блоке параметров **Критерий срабатывания правила** выберите вариант **Путь к файлу**.
8. Введите следующую маску: `?:\`
9. В окне **Параметры правила** нажмите на кнопку **OK**.

Kaspersky Embedded Systems Security применяет режим разрешения по умолчанию.

Формирование разрешающих правил по событиям задачи Контроль запуска программ

Чтобы создать конфигурационный файл с разрешающими правилами, сформированный по событиям задачи Контроль запуска программ, выполните следующие действия:

1. Запустите задачу Контроль запуска программ в режиме **Только статистика**, чтобы регистрировать в журнале выполнения задачи информацию обо всех запусках программ на защищаемом устройстве.

2. По завершении выполнения задачи в режиме **Только статистика** откройте журнал выполнения задачи по кнопке **Открыть журнал выполнения** в блоке **Управление** панели результатов узла **Контроль запуска программ**.

3. В окне **Журнал выполнения** нажмите на кнопку **Сформировать правила по событиям**.

   Kaspersky Embedded Systems Security создаст конфигурационный файл в формате XML со списком правил, сформированных на основе событий задачи Контроль запуска программ, отработавшей в режиме **Только статистика**. Вы можете применить этот список правил в задаче Контроль запуска программ.

Перед применением списка правил, сформированного по событиям задачи, рекомендуется просмотреть и обработать вручную список правил, чтобы убедиться, что запуск важных файлов (например, файлов операционной системы) разрешен заданными правилами.

Все события задачи фиксируются в журнале выполнения задачи, независимо от режима работы задачи. Вы можете создать конфигурационный файл со списком правил на основе журнала, сформированного во время выполнения задачи в режиме **Активный**. Этот сценарий не рекомендуется применять, за исключением случаев экстренной необходимости, поскольку финальный список правил должен быть сформирован перед запуском задачи в режиме **Активный**, чтобы правила работали эффективно.

Экспорт правил контроля запуска программ

Чтобы экспортировать правила контроля запуска программ в конфигурационный файл, выполните следующие действия:

1. Откройте окно **Правила контроля запуска программ**.

2. Нажмите на кнопку **Экспортировать в файл**.

   Откроется стандартное окно Microsoft Windows.

3. В открывшемся окне укажите файл, в который вы хотите экспортировать правила. Если такого файла не существует, то он будет создан. Если файл с указанным именем уже существует, при экспорте правил его содержимое будет перезаписано.

4. Нажмите на кнопку **Сохранить**.

   Параметры правил будут экспортированы в указанный файл.

Импорт правил контроля запуска программ из XML-файла

Чтобы импортировать правила контроля запуска программ, выполните следующие действия:

1. Откройте окно **Правила контроля запуска программ**.
2. Нажмите на кнопку **Добавить**.
3. В контекстном меню кнопки выберите пункт **Импортировать правила из файла формата XML**.
4. Укажите способ добавления импортируемых правил. Для этого выберите один из пунктов контекстного меню кнопки **Импортировать правила из файла формата XML**:

   - **Добавить правила к существующим**, если требуется, чтобы импортируемые правила были добавлены в список существующих правил. Правила с одинаковыми параметрами дублируют друг друга.
   - **Заменить существующие правила**, если вы хотите, чтобы импортируемые правила заменили существующие правила.
   - **Объединить правила с существующими**, если вы хотите, чтобы импортируемые правила были добавлены в список существующих правил. Правила с дублирующими параметрами не добавляются; если хотя бы один параметр правила уникален, правило добавляется.

   Откроется стандартное окно Microsoft Windows **Открыть**.
5. В окне **Открыть** выберите XML-файл, содержащий правила контроля запуска программ.
6. Нажмите на кнопку **Открыть**.

Импортированные правила отобразятся в окне **Правила контроля запуска программ**.

Удаление правил контроля запуска программ

Чтобы удалить правила контроля запуска программ, выполните следующие действия:

1. Откройте окно **Правила контроля запуска программ**.
2. В списке выберите правила, которые требуется удалить.
3. Нажмите на кнопку **Удалить выбранные**.
4. Нажмите на кнопку **Сохранить**.

Выбранные правила контроля запуска программ будут удалены.

Настройка задачи Формирование правил контроля запуска программ

Чтобы настроить параметры задачи Формирование правил контроля запуска программ, выполните следующие действия:

1. Откройте окно **Параметры задачи** для задачи **Формирование правил контроля запуска программ**.
2. Настройте следующие параметры:
   - На закладке **Общие**:
     - Укажите **Префикс для названий правил**.
     - Настройте область применения разрешающих правил.
   - На закладке **Действия** укажите действия, которые должна выполнять программа Kaspersky Embedded Systems Security:
     - при формировании разрешающих правил;
     - по завершении задачи.
   - На закладках **Расписание** и **Дополнительно** настройте расписание запуска задачи.
   - На закладке **Запуск с правами** настройте запуск задачи с правами учетной записи.
3. В окне **Параметры задачи** нажмите на кнопку **OK**.

Kaspersky Embedded Systems Security немедленно применит новые значения параметров в выполняющейся задаче. Данные о дате и времени изменения параметров, а также значения параметров задачи до и после их изменения.

Ограничение области действия задачи

Чтобы ограничить область действия задачи Формирование правил контроля запуска программ, выполните следующие действия:

1. Откройте окно **Параметры задачи** для задачи **Формирование правил контроля запуска программ**.
2. Выберите способ создания разрешающих правил:
   - **Создавать разрешающие правила на основе запущенных программ**
   - **Создавать разрешающие правила для программ из папок**
3. В окне **Параметры задачи** нажмите на кнопку **OK**.

Настроенные параметры будут сохранены.

Действия при автоматическом формировании правил

Чтобы настроить действия Kaspersky Embedded Systems Security во время выполнения задачи Формирование правил контроля запуска программ, выполните следующие действия:

1. Откройте окно **Параметры задачи** для задачи **Формирование правил контроля запуска программ**.

2. Выберите закладку **Параметры**.

3. В блоке **При формировании разрешающих правил** настройте следующие параметры:

   - **Использовать цифровой сертификат**
   - **Использовать заголовок и отпечаток цифрового сертификата**
   - **Если сертификат отсутствует, использовать**
     - **хеш SHA256** В качестве критерия срабатывания разрешающего правила контроля запуска программ устанавливается контрольная сумма файла, на основе которого формируется правило. В дальнейшем программа будет разрешать запуск программ, запускаемых файлами с указанной контрольной суммой.
     - **путь к файлу** В качестве критерия срабатывания разрешающего правила контроля запуска программ устанавливается путь к файлу, на основе которого формируется правило. В дальнейшем программа будет разрешать запуск программ теми файлами, которые находятся в папках, указанных в таблице **Создавать разрешающие правила для программ из папок** в разделе **Настройка**.
   - **Использовать хеш SHA256**
   - **Формировать правила для пользователя или группы пользователей**.

4. В окне **Параметры задачи** нажмите на кнопку **OK**.

Настроенные параметры будут сохранены.

Действия по завершении автоматического формирования правил

Чтобы настроить действия Kaspersky Embedded Systems Security по завершении выполнения задачи Формирование правил контроля запуска программ, выполните следующие действия:

1. Откройте окно **Параметры задачи** для задачи **Формирование правил контроля запуска программ**.

2. Выберите закладку **Параметры**.

3. В блоке **По завершении задачи** настройте следующие параметры:

   - **Добавлять разрешающие правила в список правил контроля запуска программ**
   - **Принцип добавления**
   - **Экспортировать разрешающие правила в файл**
   - **Добавлять информацию о компьютере в имя файла**

4. В окне **Параметры задачи** нажмите на кнопку **OK**.

Настроенные параметры будут сохранены.

Управление контролем запуска программ с помощью веб-плагина

Чтобы настроить задачи контроля запуска программ с помощью веб-плагина, выполните следующие действия:

1. В главном окне веб-консоли выберите **Устройства** → **Политики и профили**.
2. Выберите политику, которую вы хотите настроить.
3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.
4. Выберите раздел **Контроль активности на компьютерах**.
5. Нажмите на кнопку **Параметры** в подразделе **Контроль запуска программ**.
6. Настройте параметры, приведены в следующей таблице.

Параметры задачи Контроль запуска программ

Параметр	Описание
Режим работы	В раскрывающемся списке вы можете выбрать один из следующих режимов работы задачи Контроль запуска программ: • **Активный** Kaspersky Embedded Systems Security использует определенные правила контроля запуска всех программ. • **Только статистика** Kaspersky Embedded Systems Security не использует правила контроля запуска программ, а только фиксирует в журнале выполнения задач информацию о запусках программ. Разрешен запуск всех программ. Вы можете использовать этот режим для формирования списка правил контроля запуска программ на основе информации о заблокированных запусках программ, зарегистрированной в журнале выполнения задачи. По умолчанию задача Контроль запуска программ запускается в режиме **Только статистика**.
Обрабатывать повторные запуски контролируемых программ по схеме обработки первого запуска	Флажок включает или выключает контроль повторного запуска программ на основе информации о событиях, хранящейся в кеше. Если флажок установлен, Kaspersky Embedded Systems Security разрешает или запрещает следующие запуски программ в зависимости от заключения задачи насчет первого запуска программы. Например, если первый запуск программы был разрешен правилами контроля запуска программ, запись об этом сохраняется в кеше, и повторный запуск этой программы будет разрешен без повторной проверки. Если флажок снят, Kaspersky Embedded Systems Security проверяет программу при каждой попытке ее запуска. По умолчанию флажок установлен.
Запрещать запуск командных интерпретаторов без команды к исполнению	Если флажок установлен, Kaspersky Embedded Systems Security запрещает запуск командного интерпретатора, даже если запуск интерпретатора разрешен. Запуск командного интерпретатора без команд разрешается только при выполнении обоих условий: • Запуск командного интерпретатора разрешен. • Исполняемая команда разрешена.

	Если флажок снят, Kaspersky Embedded Systems Security учитывает только разрешающие правила при запуске командного интерпретатора. Запуск блокируется, если не применимо ни одно разрешающее правило или выполняемый процесс не является доверенным в KSN. Если применимо разрешающее правило или если процесс является доверенным в KSN, запуск командного интерпретатора разрешается как с исполняемой командой, так и без нее. Kaspersky Embedded Systems Security работает со следующими командными интерпретаторами: • cmd.exe; • powershell.exe; • python.exe; • perl.exe. По умолчанию флажок снят.
Использовать правила для исполняемых файлов	Флажок включает или выключает контроль запуска исполняемых файлов. Если флажок установлен, Kaspersky Embedded Systems Security разрешает или запрещает запуск исполняемых файлов на основе заданных правил, в параметрах которых указана область применения **Исполняемые файлы**. Если флажок снят, Kaspersky Embedded Systems Security не контролирует запуск исполняемых файлов с помощью заданных правил. Запуск исполняемых файлов разрешен. По умолчанию флажок установлен.
Контролировать загрузку DLL-модулей	Флажок включает или выключает контроль загрузки DLL-модулей. Если флажок установлен, Kaspersky Embedded Systems Security разрешает или запрещает загрузку DLL-модулей на основе заданных правил, в параметрах которых указана область применения **Исполняемые файлы**. Если флажок снят, Kaspersky Embedded Systems Security не контролирует загрузку DLL-модулей с помощью заданных правил. Загрузка DLL-модулей разрешена. Флажок доступен, если установлен флажок **Использовать правила для исполняемых файлов**. По умолчанию флажок снят.
Использовать правила для скриптов и пакетов MSI	Флажок включает или выключает запуск скриптов и пакетов MSI. Если флажок установлен, Kaspersky Embedded Systems Security разрешает или запрещает запуск скриптов и пакетов MSI с помощью заданных правил, в параметрах которых указана область применения Скрипты и пакеты MSI. Если флажок снят, Kaspersky Embedded Systems Security не контролирует запуск скриптов и пакетов MSI с помощью заданных правил. Запуск скриптов и пакетов MSI разрешен. По умолчанию флажок установлен.
Запрещать запуск программ, недоверенных в KSN	Флажок включает или выключает контроль запуска программ согласно данным о репутации программ в KSN.

	Если флажок установлен, Kaspersky Embedded Systems Security запрещает запуск программ, недоверенных в KSN. Разрешающие правила контроля запуска программ, применимые к недоверенным в KSN программам, не срабатывают. Установка флажка обеспечивает дополнительную защиту от вредоносных программ. Если флажок снят, Kaspersky Embedded Systems Security не учитывает репутацию программ, не являющихся доверенными в KSN, и разрешает или запрещает их запуск в соответствии с правилами, применимыми к этим программам. По умолчанию флажок снят.
Разрешать запуск программ, доверенных в KSN	Флажок включает или выключает контроль запуска программ согласно данным о репутации программ в KSN. Если флажок установлен, Kaspersky Embedded Systems Security разрешает запуск программ, доверенных в KSN. Запрещающие правила контроля запуска программ, под которые подпадают доверенные в KSN программы, имеют больший приоритет: если программа признана доверенной службами KSN, но запрещена правилами контроля запуска программ, запуск такой программы будет заблокирован. Если флажок снят, Kaspersky Embedded Systems Security не учитывает репутацию программ, доверенных в KSN, и разрешает или запрещает их запуск в соответствии с правилами, применимыми к этим программам. По умолчанию флажок снят.
Правила	Настройте разрешающие и запрещающие правила для задачи контроля запуска программ.
Контроль пакетов установки	Можно добавлять доверенные пакеты установки.
Управление задачами	Вы можете настроить расписание запуска задачи.

Контроль устройств

Этот раздел содержит информацию о задаче Контроль устройств и инструкции о том, как настроить параметры этой задачи.

О задаче Контроль устройств

Kaspersky Embedded Systems Security контролирует регистрацию и использование внешних устройств и CD/DVD-дисководов в целях защиты устройства от угроз безопасности, которые могут возникнуть во время файлового обмена с USB-подключаемыми флеш-накопителями или внешними устройствами другого типа.

Kaspersky Embedded Systems Security контролирует подключение следующих типов внешних устройств:

- USB-подключаемые флеш-накопители;
- устройства чтения CD/DVD-дисков;
- USB-подключаемые устройства чтения гибких дисков;
- USB-подключаемые сетевые адаптеры;
- USB-подключаемые мобильные устройства MTP.

Kaspersky Embedded Systems Security сообщает обо всех устройствах, подключенных по USB, с помощью соответствующего события в журнале событий и в журнале выполнения задачи. Описание события включает тип устройства и путь подключения При запуске задачи Контроль устройств Kaspersky Embedded Systems Security проверяет и перечисляет все устройства, подключенные по USB. Уведомления можно настроить в блоке параметров уведомлений Kaspersky Security Center.

Задача Контроль устройств отслеживает попытки подключения внешних устройств к защищаемому устройству по USB и блокирует их подключение, если не находит разрешающих правил для этих устройств. После блокировки соединения устройство становится недоступно.

Программа присваивает каждому подключаемому внешнему устройству один из следующих статусов:

- *Доверенное*. Устройство, обмен данными с которым разрешен. При формировании правила значение *Путь к экземпляру устройства* подпадает под область применения хотя бы одного правила.
- *Недоверенное*. Устройство, обмен данными с которым запрещен. Путь к экземпляру такого устройства не подпадает под область применения разрешающих правил.

Вы можете создать разрешающие правила для внешних устройств, обмен данными с которыми вы хотите разрешить, с помощью задачи Формирование правил контроля устройств. Вы также можете расширять область применения уже созданных разрешающих правил. Вы не можете создавать разрешающие правила вручную.

Kaspersky Embedded Systems Security идентифицирует регистрируемое в системе внешнее устройство по значению пути к экземпляру устройства. Путь к экземпляру устройства является уникальным признаком для каждого устройства. Информация о пути к экземпляру устройства содержится в свойствах внешнего устройства в операционной системе Windows и определяется Kaspersky Embedded Systems Security в момент создания разрешающих правил автоматически.

Задача Контроль устройств может выполняться в одном из двух режимов:

- **Активный** Kaspersky Embedded Systems Security контролирует с помощью правил подключение флеш-накопителей и других внешних устройств и запрещает или разрешает использование всех устройств в соответствии с принципом запрета по умолчанию и заданными разрешающими правилами. Использование доверенных внешних устройств разрешено. Использование недоверенных внешних устройств запрещено по умолчанию.

  Если внешнее устройство, которое вы считаете недоверенным, было подключено к защищаемому устройству до того, как задача Контроль устройств была запущена в активном режиме, то это устройство не будет заблокировано программой. Рекомендуется отключить недоверенное устройство вручную или перезагрузить защищаемое устройство. В противном случае принцип запрета по умолчанию не будет применен к устройству.

- **Только статистика** Kaspersky Embedded Systems Security не контролирует подключение флеш-накопителей и других внешних устройств, а только фиксирует в журнале выполнения задачи информацию о подключениях и регистрации внешних устройств на защищаемом устройстве, а также о разрешающих правилах контроля устройств, которым удовлетворяют подключаемые устройства. Использование всех внешних устройств разрешено. Этот режим установлен по умолчанию.

  Этот режим можно использовать для формирования правил на основе информации о блокировании устройств, зарегистрированной во время выполнения задачи.

О правилах контроля устройств

Kaspersky Embedded Systems Security не использует разрешающие правила для MTP-подключаемых мобильных устройств.

Правила создаются индивидуально для каждого устройства, подключенного в данный момент или подключавшегося ранее к защищаемому устройству, если данные об этом устройстве сохранились в системе.

Для формирования разрешающих правил контроля устройств можно:

- использовать задачу Формирование правил контроля устройств;
- запустить задачу Контроль устройств в режиме Только статистика;
- использовать данные системы о подключавшихся устройствах;
- расширить область применения уже созданных правил.

Максимальное количество правил контроля устройств, которое поддерживает Kaspersky Embedded Systems Security, составляет 3072.

Правила контроля устройств описаны ниже.

Тип правила

Тип правила - всегда *разрешающее*. Задача Контроль устройств по умолчанию блокирует подключение всех флеш-накопителей и других внешних устройств, если они не подпадают под область действия ни одного разрешающего правила.

Критерий срабатывания и область применения правила

Правила контроля устройств идентифицируют подключаемые флеш-накопители и другие внешние устройства по значению параметра *Путь к экземпляру устройства*. Путь к экземпляру устройства является уникальным идентификатором, который система присваивает устройству в момент его подключения и регистрации в качестве внешнего устройства или устройства чтения CD/DVD-дисков (например, IDE или SCSI).

Kaspersky Embedded Systems Security контролирует подключение устройств чтения CD/DVD дисков вне зависимости от шины подключения. При монтировании таких устройств по USB, операционная система регистрирует два значения пути к экземпляру устройства: для внешнего устройства и для устройства чтения CD/DVD-дисков (например, IDE или SCSI). Для корректного подключения таких устройств требуется наличие разрешающих правил для каждого значения пути к экземпляру устройства.

Kaspersky Embedded Systems Security автоматически определяет путь к экземпляру устройства и разбивает найденное значение на следующие составляющие:

- производитель устройства (VID);
- тип контроллера устройства (PID);
- серийный номер устройства.

Вы не можете задавать путь к экземпляру устройства вручную. Заданные в свойствах разрешающего правила критерии срабатывания правила определяют область применения этого правила. По умолчанию в область применения только что созданного разрешающего правила включено одно устройство, на основе свойств которого Kaspersky Embedded Systems Security сформировал разрешающее правило. Вы можете изменять значения параметров созданного правила с помощью маски, чтобы расширить область применения правила.

Данные исходного устройства

Данные устройства, на основе которых программа Kaspersky Embedded Systems Security сформировала разрешающее правило, отображаются в свойствах каждого правила.

Данные исходного устройства содержат следующую информацию:

- **Путь к экземпляру устройства**. На основании этого свойства Kaspersky Embedded Systems Security определяет критерий срабатывания правила и заполняет следующие поля: **Производитель (VID)**, **Тип контроллера (PID)**, **Серийный номер** в блоке **Область применения правила** окна **Параметры правила**.
- **Адаптированное имя**. Имя, которое задается в свойствах устройства производителем.

При создании правила Kaspersky Embedded Systems Security автоматически определяет исходные значения для устройства. В дальнейшем вы можете использовать эти значения, чтобы определить, на основе данных какого устройства было создано правило. Данные исходного устройства недоступны для редактирования.

Описание

Вы можете добавить дополнительную информацию для каждого созданного правила контроля устройств в поле **Комментарий**, например, название подключаемого флеш-накопителя или имя его владельца. Комментарий отображается в соответствующем поле в окне **Правила контроля устройств**.

Комментарий и данные исходного устройства не учитываются при работе правила и служат только для упрощения идентификации устройств и правил пользователем.

О формировании правил контроля устройств

Вы можете импортировать списки разрешающих правил контроля устройств из XML-файлов, сформированных автоматически в ходе выполнения задачи Контроль устройств или задачи Формирование правил контроля устройств.

По умолчанию Kaspersky Embedded Systems Security запрещает подключение любых флеш-накопителей и других внешних устройств, которые не подпадают под действие заданных правил контроля устройств.

Цели и сценарии формирования правил контроля устройств

Сценарий формирования списка правил	Решаемая задача
Задача Формирование правил контроля устройств	• Создать разрешающие правила для уже использовавшихся доверенных устройств перед первым запуском задачи Контроль устройств. • Сформировать список правил для доверенных устройств в сети защищаемых устройств.
Создание правил на основе данных системы	Создать разрешающие правила для внешних устройств, данные о которых хранятся в системе.
Формирование правил по данным о подключенных в текущий момент устройствах	Обновление списка существующих правил, если нужно разрешить использование небольшого количества новых внешних устройств.
Режим **Только статистика** задачи Контроль устройств	Добавить разрешающие правила для большого количества доверенных устройств.

Использование задачи Формирование правил контроля устройств

XML-файл, сформированный по завершении задачи Формирование правил контроля устройств, содержит разрешающие правила для флеш-накопителей и других внешних устройств, данные о подключении которых сохранились в системе.

Используйте этот способ, чтобы учесть при формировании правил данные обо всех когда-либо подключавшихся внешних устройствах, сохранившиеся в системах на всех защищаемых устройствах сети, или данные только об устройствах, подключенных в настоящее время. Задача также учитывает все внешние устройства, подключенные в момент выполнения задачи. По завершении выполнения групповой задачи, Kaspersky Embedded Systems Security формирует списки разрешающих правил для всех зарегистрированных в сети внешних устройств и сохраняет эти списки в XML-файл в указанной папке. Далее вы можете вручную импортировать сформированные правила в свойства задачи Контроль устройств. В отличие от задачи на защищаемом устройстве, в политике невозможно настроить автоматическое добавление созданных правил в список правил контроля устройств по завершении групповой задачи Формирование правил контроля устройств.

Рекомендуется использовать этот сценарий для формирования списка разрешающих правил перед первым запуском задачи Контроль устройств, чтобы сформированные разрешающие правила учитывали все доверенные внешние устройства, используемые на защищаемом устройстве.

Использование данных системы обо всех подключаемых устройствах

В ходе выполнения задачи Kaspersky Embedded Systems Security получает данные системы обо всех внешних устройствах, подключавшихся ранее и подключенных к защищаемому устройству в данный момент, и отображает обнаруженные устройства в списке в окне **Сформировать правила на основе данных системы**.

Для каждого обнаруженного устройства Kaspersky Embedded Systems Security определяет производителя (VID), тип контроллера (PID), адаптированное имя, серийный номер и путь к экземпляру устройства. Можно сформировать разрешающие правила для любого внешнего устройства, данные о котором хранятся в системе, и сразу добавить новые правила в список правил контроля устройств.

При использовании этого сценария Kaspersky Embedded Systems Security формирует разрешающие правила для внешних устройств, подключавшихся ранее или подключенных в текущий момент к защищаемому устройству, на котором установлена программа Kaspersky Security Center.

Рекомендуется использовать этот сценарий для обновления списка существующих правил, если нужно разрешить использование небольшого количества новых внешних устройств.

Использование данных о подключенных в текущий момент устройствах

При использовании этого сценария Kaspersky Embedded Systems Security формирует разрешающие правила только для внешних устройств, подключенных в текущий момент. Вы можете выбрать одно или несколько внешних устройств, для которых вы хотите сформировать разрешающие правила.

Использование задачи Контроль устройств в режиме Только статистика

XML-файл, полученный по завершении задачи Контроль устройств в режиме **Только статистика**, формируется на основе журнала выполнения задачи.

В ходе выполнения задачи Kaspersky Embedded Systems Security фиксирует информацию обо всех подключениях флеш-накопителей и других внешних устройств к защищаемому устройству в журнале выполнения задачи. Вы можете сформировать разрешающие правила по событиям задачи и экспортировать их в XML-файл. Перед запуском задачи в режиме **Только статистика** рекомендуется настроить период выполнения задачи так, чтобы за указанный временной промежуток выполнились все возможные подключения внешних устройств к защищаемому устройству.

Рекомендуется использовать этот сценарий для обновления существующего списка правил, если нужно разрешить использование большого количества новых внешних устройств.

Если формирование списка правил по этому сценарию выполняется на эталонной машине, вы можете применить сформированный список разрешающих правил при настройке задачи Контроль устройств в Kaspersky Security Center. Таким образом вы сможете разрешать использование внешних устройств, подключенных к эталонной машине, на защищаемых устройствах.

О задаче Формирование правил контроля устройств

Задача Формирование правил контроля устройств позволяет автоматически формировать список разрешающих правил для подключения флеш-накопителей и других внешних устройств на основе данных системы обо всех внешних устройствах, которые ранее подключались к защищаемому устройству.

По завершении выполнения задачи Kaspersky Embedded Systems Security создает конфигурационный файл в формате XML со списком разрешающих правил для обнаруженных внешних устройств или сразу добавляет сформированные правила в задачу Контроль устройств в зависимости от параметров задачи Формирование правил контроля устройств. В дальнейшем программа будет разрешать подключение устройств, для которых были автоматически сформированы разрешающие правила.

Сформированные и добавленные в задачу правила отображаются в окне **Правила контроля устройств**.

Параметры по умолчанию для задачи Контроль устройств

По умолчанию задача Контроль устройств имеет параметры, описанные в таблице ниже. Вы можете изменять значения этих параметров.

Параметры по умолчанию для задачи Контроль устройств

Параметр	Значение по умолчанию	Описание
Режим работы	**Только статистика**	Задача фиксирует в журнале выполнения события запрета и разрешения подключения внешних устройств в соответствии с заданными правилами. Фактическая блокировка использования внешних устройств не выполняется. Вы можете выбрать режим **Активный** для защиты устройства, чтобы применять фактическую блокировку использования внешних устройств.
Разрешать использование всех запоминающих устройств, если задача Контроль устройств не выполняется	Не применяется	Kaspersky Embedded Systems Security запрещает использование внешних устройств вне зависимости от статуса выполнения задачи Контроль устройств. Это обеспечивает максимальную защиту от угроз компьютерной безопасности, возникающих при файловом обмене с внешними устройствами. Вы можете настраивать параметр таким образом, чтобы программа Kaspersky Embedded Systems Security разрешала использование всех внешних устройств, если задача Контроль устройств не выполняется.
Расписание запуска задачи	Время первого запуска не задано.	Задача Контроль устройств не запускается автоматически при запуске программы Kaspersky Embedded Systems Security. Вы можете настроить запуск задачи по расписанию.

Параметры задачи Формирование правил контроля устройств по умолчанию

Параметр	Значение по умолчанию	Описание
Режим генерации	**Учитывать данные системы обо всех когда-либо подключавшихся устройствах**	Режим работы задачи. Можно выбрать режим **Учитывать данные только об устройствах, подключенных в текущий момент**.
Действия по завершении задачи	Разрешающие правила добавляются в список правил задачи Контроль устройств; новые правила объединяются с существующими правилами; дублирующие правила удаляются.	Вы можете добавлять правила к уже существующим правилам без объединения и без удаления дублирующих правил или заменять существующие правила новыми разрешающими правилами, а также настроить параметры экспорта разрешающих правил в файл.
Расписание запуска задачи	Время первого запуска не задано.	Задача Формирование правил контроля устройств не запускается автоматически при запуске программы Kaspersky Embedded Systems Security. Вы можете запустить задачу вручную или настроить запуск задачи по расписанию.

Управление контролем устройств с помощью Плагина управления

В этом разделе описана навигация в интерфейсе Плагина управления и управление подключением внешних устройств ко всем защищаемым устройствам в сети с помощью списков правил в Kaspersky Security Center для групп защищаемых устройств.

Навигация

В этом разделе описан переход к требуемым параметрам задачи с помощью интерфейса.

Переход к параметрам политики для задачи Контроль устройств

Чтобы перейти к параметрам задачи Контроль устройств в политике Kaspersky Security Center, выполните следующие действия:

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой вы хотите настроить задачу.
3. Выберите закладку **Политики**.
4. Откройте окно свойств политики двойным щелчком мыши на имени политики, которую вы хотите настроить.
5. В открывшемся окне **Свойства: <Имя политики>** перейдите в раздел **Контроль активности на серверах**.
6. Нажмите на кнопку **Настройка** в подразделе **Контроль устройств**.

   Откроется окно **Контроль устройств**.

7. Настройте политику в соответствии с вашими требованиями.

Переход к списку правил контроля устройств

Чтобы перейти к списку правил контроля устройств в Kaspersky Security Center, выполните следующие действия:

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой вы хотите настроить задачу.
3. Выберите закладку **Политики**.
4. Откройте окно свойств политики двойным щелчком мыши на имени политики, которую вы хотите настроить.
5. В открывшемся окне **Свойства: <Имя политики>** перейдите в раздел **Контроль активности на серверах**.
6. Нажмите на кнопку **Настройка** в подразделе **Контроль устройств**.

   Откроется окно **Контроль устройств**.
7. На закладке **Общие** нажмите на кнопку **Список правил**.

   Откроется окно **Правила контроля устройств**.
8. Настройте политику в соответствии с вашими требованиями.

Переход к мастеру создания задачи Формирование правил контроля устройств и ее свойствам

Чтобы создать задачу Формирование правил контроля устройств, выполните следующие действия:

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой вы хотите настроить задачу.
3. Выберите закладку **Задачи**.
4. Нажмите на кнопку **Создать задачу**.

   Откроется окно **Мастер создания задачи**.
5. Выберите задачу **Формирование правил контроля устройств**.
6. Нажмите на кнопку **Далее**.

   Откроется окно **Настройка**.

Чтобы настроить задачу Формирование правил контроля устройств, выполните следующие действия:

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой вы хотите настроить задачу.
3. Выберите закладку **Задачи**.
4. Выберите название задачи в списке задач Kaspersky Security Center двойным щелчком мыши.

   Откроется окно **Свойства: Формирование правил контроля устройств**.

Дополнительную информацию о настройке задачи см. в разделе Настройка задачи Формирование правил контроля устройств.

Настройка задачи Контроль устройств

Чтобы настроить параметры задачи Контроль устройств, выполните следующие действия:

1. Откройте окно **Контроль устройств**.
2. На закладке **Общие** настройте следующие параметры задачи:
   - В блоке **Режим работы** выберите один из следующих режимов работы задачи:
     - **Активный**

       Если внешнее устройство, которое вы считаете недоверенным, было подключено к защищаемому устройству до того, как задача Контроль устройств была запущена в активном режиме, то это устройство не будет заблокировано программой. Рекомендуется отключить недоверенное устройство вручную или перезагрузить защищаемое устройство. В противном случае принцип запрета по умолчанию не будет применен к устройству.

     - **Только статистика**
   - Снимите или установите флажок **Разрешать использование всех запоминающих устройств, если задача Контроль устройств не выполняется**.
3. Нажмите на кнопку **Список правил**, чтобы изменить список правил контроля устройств.
4. Если требуется, настройте расписание запуска задачи на закладке **Управление задачей**.
5. Нажмите на кнопку OK в окне **Контроль устройств**.

Kaspersky Embedded Systems Security немедленно применит новые значения параметров в выполняющейся задаче. Данные о дате и времени изменения параметров, а также значения параметров задачи до и после изменения будут сохранены в журнале системного аудита.

Настройка задачи Формирование правил контроля устройств

Чтобы настроить задачу Формирование правил контроля устройств, выполните следующие действия:

1. Откройте окно **Свойства: Формирование правил контроля устройств**.

2. В разделе **Уведомления** настройте параметры уведомлений о событиях задачи.

   Подробная информация о настройке параметров в этом разделе приведена в *Справке Kaspersky Security Center*.

3. В разделе **Настройка** можно настроить следующие параметры:

   - Выберите режим работы: учитывать данные системы обо всех когда-либо подключавшихся внешних устройствах или только о подключенных в настоящий момент внешних устройствах.
   - Настройте параметры для конфигурационных файлов со списком разрешающих правил, которые Kaspersky Embedded Systems Security создает по завершении задачи.

4. В разделе **Расписание** настройте параметры расписания задачи (вы можете настраивать расписание всех задач, кроме задачи Откат обновления баз программы).

5. В разделе **Учетная запись** укажите учетную запись, с правами которой будет выполняться задача.

6. Если требуется, в разделе **Исключения** из области действия задачи укажите объекты, которые хотите исключить из области действия задачи.

   Подробная информация о настройке параметров в этом разделе приведена в *Справке Kaspersky Security Center*.

7. В окне **Свойства: <Название задачи>** нажмите на кнопку **ОК**.

   Настроенные параметры групповых задач будут сохранены.

Настройка правил контроля устройств в Kaspersky Security Center

В этом разделе описано формирование списка правил на основе различных критериев, а также создание разрешающих и запрещающих правил вручную с помощью задачи Контроль устройств.

Формирование разрешающих правил на основе данных системы в политике Kaspersky Security Center

*Чтобы задать разрешающие правила с помощью параметра **Сформировать правила на основе данных системы** задачи Контроль устройств, выполните следующие действия:*

1. Если требуется, подключите к защищаемому устройству с установленной Консолью администрирования Kaspersky Security Center новое внешнее устройство, использование которого вы хотите разрешить.

2. Откройте окно **Правила контроля устройств**.

3. Нажмите на кнопку **Добавить** и в контекстном меню кнопки выберите пункт **Сформировать правила на основе данных системы**.

4. Выберите устройство в списке устройств в окне **Сформировать правила на основе данных системы**.

5. Нажмите на кнопку **Добавить правила для выбранных устройств**.

6. Нажмите на кнопку **Сохранить** в окне **Правила контроля устройств**.

Список правил в задаче Контроль устройств будет дополнен новыми правилами, сформированными на основе системных данных защищаемого устройства, на котором установлена Консоль администрирования Kaspersky Security Center.

Формирование правил для подключенных устройств

*Чтобы задать разрешающие правила с помощью параметра **Сформировать правила для устройств, подключенных в текущий момент** задачи Контроль устройств, выполните следующие действия:*

1. Откройте окно **Правила контроля устройств**.

2. Нажмите на кнопку **Добавить** и в контекстном меню кнопки выберите пункт **Сформировать правила для устройств, подключенных в текущий момент**.

   Откроется окно **Сформировать правила на основе данных системы**.

3. В списке обнаруженных устройств, подключенных к защищаемому устройству, выберите устройства, для которых вы хотите сформировать разрешающие правила.

4. Нажмите на кнопку **Добавить правила для выбранных устройств**.

5. Нажмите на кнопку **Сохранить** в окне **Правила контроля устройств**.

Список правил в задаче Контроль устройств будет дополнен новыми правилами, сформированными на основе системных данных защищаемого устройства, на котором установлена Консоль администрирования Kaspersky Security Center.

Импорт правил из отчета Kaspersky Security Center о заблокированных устройствах

Можно импортировать данные о заблокированных попытках подключения устройств из отчета, сформированного в Kaspersky Security Center по результатам выполнения задачи Контроль устройств в режиме **Только статистика**, и применить эти данные для формирования списка разрешающих правил контроля устройств в настраиваемой политике.

При формировании отчета о событиях, возникающих в ходе выполнения задачи Контроль устройств, вы можете отследить, подключение каких устройств будет блокироваться.

Чтобы задать разрешающие правила подключения устройств для группы защищаемых устройств на основе отчета Kaspersky Security Center о заблокированных устройствах, выполните следующие действия:

1. В свойствах политики в разделе **Уведомления о событиях** убедитесь, что выполняются следующие условия:

   - Для событий с уровнем важности **Критическое событие** срок хранения событий *Обнаружено и запрещено недоверенное устройство* в журнале выполнения задачи превышает запланированный период выполнения задачи в режиме **Только статистика** (значение по умолчанию – 30 дней).

   - Для событий с уровнем важности **Предупреждение** срок хранения событий *Только статистика: обнаружено недоверенное устройство* в журнале выполнения задачи превышает запланированный

период выполнения задачи в режиме **Только статистика** (значение по умолчанию – 30 дней).

По завершении периода хранения событий, информация о зарегистрированных событиях будет удалена и не попадет в файл отчета. Перед запуском задачи Контроль устройств в режиме **Только статистика** убедитесь, что время выполнения задачи не превышает установленное время хранения указанных событий.

2. Запустите задачу Контроль устройств в режиме **Только статистика**.

   a. В Kaspersky Security Center в рабочей области узла **Сервер администрирования** выберите закладку **События**.

   b. Нажмите на кнопку **Создать выборку** и создайте выборку событий по критерию *Обнаружено и запрещено недоверенное устройство*. Просмотрите, подключения каких устройств заблокированы задачей Контроль устройств.

   c. В панели результатов созданной выборки перейдите по ссылке **Экспортировать события в файл**, чтобы сохранить отчет о заблокированных подключениях в файл формата TXT.

Перед импортом и применением сформированного отчета в политике убедитесь, что отчет содержит данные только о тех устройствах, подключение которых вы хотите разрешить.

3. Импортируйте данные о заблокированных попытках подключения устройств в задачу Контроль устройств.

   a. Откройте окно **Правила контроля устройств**.

   b. Нажмите на кнопку **Добавить** и в контекстном меню кнопки выберите пункт **Импортировать правила из файла отчета KSC о заблокированных устройствах**.

   c. Выберите принцип добавления правил из списка, созданного на основе отчета Kaspersky Security Center, к списку уже заданных правил контроля устройств:

      - **Добавить правила к существующим**, если требуется, чтобы импортируемые правила были добавлены в список существующих правил. Правила с одинаковыми параметрами дублируют друг друга.

      - **Заменить существующие правила**, если вы хотите, чтобы импортируемые правила заменили существующие правила.

      - **Объединить правила с существующими**, если вы хотите, чтобы импортируемые правила были добавлены в список существующих правил. Правила с дублирующими параметрами не добавляются; если хотя бы один параметр правила уникален, правило добавляется.

   d. В открывшемся стандартном окне Windows выберите файл формата TXT, в который были экспортированы события из отчета о заблокированных устройствах.

   e. Нажмите на кнопку **Сохранить** в окне **Правила контроля устройств**.

4. Нажмите на кнопку **ОК** в окне **Контроль устройств**.

Правила, созданные на основе отчета Kaspersky Security Center о заблокированных устройствах, будут добавлены к списку правил в политике контроля устройств.

Создание правил с помощью задачи Формирование правил контроля устройств

Чтобы задать разрешающие правила контроля устройств для группы защищаемых устройств с помощью задачи Формирование правил контроля устройств, выполните следующие действия:

1. Откройте окно **Настройка** в мастере создания задачи.
2. Настройте следующие параметры:
   - В блоке **Режим**:
     - **Учитывать данные системы обо всех когда-либо подключавшихся устройствах**
     - **Учитывать данные только об устройствах, подключенных в текущий момент**
   - В блоке **После завершения задачи**:
     - **Добавлять разрешающие правила в список правил контроля устройств**
     - **Принцип добавления**
     - **Экспортировать разрешающие правила в файл**
     - **Добавлять информацию о сервере в имя файла**
3. Нажмите на кнопку Далее.
4. В окне **Расписание** укажите параметры запуска задачи по расписанию.
5. Нажмите на кнопку Далее.
6. В окне Выбор учетной записи для запуска задачи укажите требуемую учетную запись.
7. Нажмите на кнопку Далее.
8. Укажите название задачи.
9. Нажмите на кнопку Далее.

   Название задачи не должно быть длиннее 100 символов и не должно содержать следующие символы: " * < > & \ : |

   Откроется окно Завершение создания задачи.
10. По завершении работы мастера можно запустить задачу, установив флажок Запустить задачу после завершения работы мастера.
11. Нажмите на кнопку Завершить, чтобы завершить создание задачи.

12. На закладке Задачи в рабочей области настраиваемой группы защищаемых устройств в списке групповых задач выберите созданную задачу Формирование правил контроля устройств.

13. Нажмите на кнопку Запустить для запуска задачи.

    По завершении задачи автоматически сформированные списки разрешающих правил будут сохранены в папке общего доступа в файлах формата XML.

    При применении политики контроля устройств в сети убедитесь, что для всех защищаемых устройств настроен доступ к папке. Если применение сетевой папки общего доступа не предусмотрено политикой организации, рекомендуется запускать задачу Формирование правил контроля устройств в тестовой группе защищаемых устройств или на эталонной машине организации.

Добавление сформированных правил в список правил контроля устройств

Чтобы добавить сформированные списки разрешающих правил в задачу Контроль устройств, выполните следующие действия:

1. Откройте окно **Правила контроля устройств**.

2. Нажмите на кнопку **Добавить**.

3. В контекстном меню кнопки **Добавить** выберите пункт **Импортировать правила из файла XML**.

4. Выберите принцип добавления автоматически сформированных разрешающих правил к списку уже заданных правил контроля устройств:

   - **Добавить правила к существующим**, если требуется, чтобы импортируемые правила были добавлены в список существующих правил. Правила с одинаковыми параметрами дублируют друг друга.

   - **Заменить существующие правила**, если вы хотите, чтобы импортируемые правила заменили существующие правила.

   - **Объединить правила с существующими**, если вы хотите, чтобы импортируемые правила были добавлены в список существующих правил. Правила с дублирующими параметрами не добавляются; если хотя бы один параметр правила уникален, правило добавляется.

5. В открывшемся стандартном окне Windows выберите файлы формата XML, созданные по завершении групповой задачи Формирование правил контроля устройств.

6. Нажмите на кнопку Открыть.

   Все сформированные правила из XML-файла добавляются в список в соответствии с выбранным принципом.

7. Нажмите на кнопку **Сохранить** в окне **Правила контроля устройств**.

8. Если вы хотите применять созданные правила контроля устройств, в свойствах политики **Контроль устройств** выберите режим выполнения задачи **Активный**.

Разрешающие правила, автоматически сформированные на основе данных системы на каждом отдельном защищаемом устройстве, будут применены на всех защищаемых устройствах в сети, на которые распространяется настраиваемая политика. Для этих защищаемых устройств программа будет разрешать подключение только тех устройств, для которых созданы разрешающие правила.

Управление Контролем устройств с помощью Консоли программы

В этом разделе описана навигация в интерфейсе Консоли программы и настройка параметров задачи на защищаемом устройстве.

Навигация

В этом разделе описан переход к требуемым параметрам задачи с помощью интерфейса.

Переход к параметрам задачи Контроль устройств

Чтобы перейти к параметрам задачи Контроль устройств в Консоли программы, выполните следующие действия:

1. В дереве Консоли программы разверните узел **Контроль компьютера**.
2. Выберите вложенный узел **Контроль устройств**.
3. В панели результатов узла **Контроль устройств** перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи**.
4. Настройте задачу в соответствии с вашими требованиями.

Переход к окну с правилами контроля устройств

Чтобы перейти к списку правил контроля устройств в Консоли программы, выполните следующие действия:

1. В дереве Консоли программы разверните узел **Контроль компьютера**.
2. Выберите вложенный узел **Контроль устройств**.
3. В панели результатов узла **Контроль устройств** перейдите по ссылке **Правила контроля устройств**.

   Откроется окно **Правила контроля устройств**.
4. Настройте список правил в соответствии с вашими требованиями.

Переход к параметрам задачи Формирование правил контроля устройств

Чтобы настроить задачу Формирование правил контроля устройств, выполните следующие действия:

1. В дереве Консоли программы разверните узел **Автоматическое формирование правил**.
2. Выберите вложенный узел **Формирование правил контроля устройств**.
3. В панели результатов узла **Формирование правил контроля устройств** перейдите по ссылке **Свойства**.
   Откроется окно **Параметры задачи**.
4. Настройте задачу в соответствии с вашими требованиями.

Настройка параметров задачи Контроль устройств

Чтобы настроить параметры задачи Контроль устройств, выполните следующие действия:

1. Откройте окно **Параметры задачи**.
2. На закладке **Общие** настройте следующие параметры задачи:
   - В блоке **Режим работы** выберите один из следующих режимов работы задачи:
     - Активный

       Если внешнее устройство, которое вы считаете недоверенным, было подключено к защищаемому устройству до того, как задача Контроль устройств была запущена в активном режиме, то это устройство не будет заблокировано программой. Рекомендуется отключить недоверенное устройство вручную или перезагрузить защищаемое устройство. В противном случае принцип запрета по умолчанию не будет применен к устройству.

     - **Только статистика**
   - Снимите или установите флажок **Разрешать использование всех запоминающих устройств, если задача Контроль устройств не выполняется**.
3. Если требуется, на закладках **Расписание** и **Дополнительно** настройте параметры запуска задачи по расписанию.
4. Чтобы изменить список правил контроля устройств, перейдите по ссылке **Правила контроля устройств** в нижней части панели результатов узла **Контроль устройств**.

Kaspersky Embedded Systems Security немедленно применит новые значения параметров в выполняющейся задаче. Данные о дате и времени изменения параметров, а также значения параметров задачи до и после изменения будут сохранены в журнале системного аудита.

Настройка правил контроля устройств

В этом разделе описано формирование, импорт и экспорт списка правил, а также создание разрешающих и запрещающих правил вручную с помощью задачи Контроль устройств.

Импорт правил контроля устройств из файла формата XML

Чтобы импортировать правила контроля устройств, выполните следующие действия:

1. Откройте окно **Правила контроля устройств**.
2. Нажмите на кнопку **Добавить**.
3. В контекстном меню кнопки выберите пункт **Импортировать правила из файла XML**.
4. Укажите способ добавления импортируемых правил. Для этого выберите один из пунктов контекстного меню кнопки **Импортировать правила из файла XML**:
   - **Добавить правила к существующим**, если вы хотите, чтобы импортируемые правила дополняли список существующих правил. Правила с одинаковыми параметрами дублируют друг друга.
   - **Заменить существующие правила**, если вы хотите, чтобы импортируемые правила добавлялись вместо существующих правил.
   - **Объединить правила с существующими**, если вы хотите, чтобы импортируемые правила дополняли список существующих правил. Правила с дублирующими параметрами не добавляются; если хотя бы один параметр правила уникален, правило добавляется.

   Откроется стандартное окно Microsoft Windows **Открыть**.
5. В окне **Открыть** выберите XML-файл, который содержит параметры правил контроля устройств.
6. Нажмите на кнопку **Открыть**.

Импортированные правила отобразятся в окне **Правила контроля устройств**.

Формирование списка правил по событиям задачи Контроль устройств

Чтобы создать конфигурационный файл со списком правил контроля устройств, сформированным по событиям задачи Контроль устройств, выполните следующие действия:

1. Запустите задачу Контроль устройств в режиме **Только статистика**, чтобы зафиксировать в журнале выполнения задачи все события подключения флеш-накопителей и других внешних устройств к защищаемому устройству.
2. По завершении выполнения задачи в режиме **Только статистика** откройте журнал выполнения задачи по кнопке **Открыть журнал выполнения** в разделе **Управление** в панели результатов узла **Контроль устройств**.
3. В окне **Журнал выполнения** нажмите на кнопку **Сформировать правила по событиям**.

Kaspersky Embedded Systems Security создаст конфигурационный файл в формате XML со списком правил на основе событий, зарегистрированных при работе задачи Контроль устройств в режиме **Только статистика**. Можно применить этот список в задаче Контроль устройств.

Перед применением списка правил, сформированного по событиям задачи, рекомендуется просмотреть, а затем вручную обработать список правил, чтобы убедиться, что подключение недоверенных устройств не разрешено заданными правилами.

При конвертации XML-файла с событиями выполнения задачи в список правил контроля устройств, программа создает разрешающие правила для всех зафиксированных событий, в том числе для событий блокирования устройств.

Все события, возникшие в ходе выполнения задачи, фиксируются в журнале выполнения задачи, независимо от режима. Вы можете создать конфигурационный файл со списком правил по результатам выполнения задачи в режиме **Активный**. Этот сценарий не рекомендуется применять, за исключением случаев экстренной необходимости, так как для эффективного выполнения задачи требуется сформировать финальную версию списка правил до запуска задачи в активном режиме.

Добавление разрешающего правила для одного или нескольких внешних устройств

В задаче контроля устройств не предусмотрена функция добавления одного правила вручную. Однако в случае, если вам необходимо добавить правила для новых внешних устройств, вы можете использовать опцию **Сформировать правила на основе данных системы**. При использовании этого сценария наполнения списка разрешающих правил программа использует данные Windows обо всех подключениях внешних устройств, когда-либо регистрировавшихся в системе, а также учитывает подключенные в текущий момент устройства.

Чтобы добавить разрешающее правило для внешних устройств, подключенных в данный момент, выполните следующие действия:

1. Откройте окно **Правила контроля устройств**.
2. Нажмите на кнопку **Добавить**.
3. В контекстном меню выберите пункт **Сформировать правила на основе данных системы**.
4. В открывшемся окне в списке обнаруженных устройств выберите устройства, использование которых вы хотите разрешить на защищаемом устройстве.
5. Нажмите на кнопку **Добавить правила для выбранных устройств**.

Новые правила будут добавлены в список правил контроля устройств.

Удаление правил контроля устройств

Чтобы удалить правила контроля устройств, выполните следующие действия:

1. Откройте окно **Правила контроля устройств**.
2. В списке правил выберите одно или несколько правил, которые вы хотите удалить.
3. Нажмите на кнопку **Удалить выбранные**.

4. Нажмите на кнопку **Сохранить**.

Выбранные правила контроля устройств будут удалены.

Экспорт правил контроля устройств

Чтобы экспортировать правила контроля устройств в конфигурационный файл, выполните следующие действия:

1. Откройте окно **Правила контроля устройств**.
2. Нажмите на кнопку **Экспортировать в файл**.

   Откроется стандартное окно Microsoft Windows.
3. В открывшемся окне укажите файл, в который вы хотите экспортировать правила. Если такого файла не существует, то он будет создан. Если файл с указанным именем уже существует, его содержимое будет перезаписано после окончания экспорта правил.
4. Нажмите на кнопку **Сохранить**.

Правила и их параметры будут экспортированы в указанный файл.

Активация и выключение правила контроля устройств

Вы можете включать и выключать применение созданных разрешающих правил контроля устройств, не удаляя их.

Чтобы включить или выключить созданное правило контроля устройств, выполните следующие действия:

1. Откройте окно **Правила контроля устройств**.
2. В списке заданных правил откройте окно **Параметры правила** двойным щелчком мыши на правиле, параметры которого хотите настроить.
3. В открывшемся окне снимите или установите флажок **Применять правило**.
4. Нажмите на кнопку **OK**.

Статус применения правила будет сохранен и отобразится для указанного правила.

Расширение области применения правил контроля устройств

Каждое автоматически созданное правило контроля устройств разрешает подключение только одного внешнего устройства. Вы можете вручную расширить область применения правила, применив маску пути к экземпляру устройства в свойствах любого заданного правила контроля устройств.

Применение маски пути к экземпляру устройства уменьшает количество разрешающих правил контроля устройств и упрощает процесс их обработки вручную. Однако расширение области применения правил может снижать эффективность контроля внешних устройств.

Чтобы применить маску пути к экземпляру устройства в свойствах правила контроля устройств, выполните следующие действия:

1. Откройте окно **Правила контроля устройств**.
2. В открывшемся окне выберите правило, на основе свойств которого вы хотите применить маску пути к экземпляру устройства.
3. Откройте окно **Параметры правила** двойным щелчком мыши на выбранном правиле контроля устройств.
4. В открывшемся окне выполните следующие действия:
   - Установите флажок **Использовать маску** рядом с полем **Тип контроллера (PID)**, если вы хотите, чтобы выбранное правило разрешало подключение всех внешних устройств с указанными данными о производителе устройства и типе контроллера.
   - Установите флажок **Использовать маску** рядом с полем **Серийный номер**, если вы хотите, чтобы выбранное правило разрешало подключение всех внешних устройств с указанными данными о производителе и серийном номере устройства.
   - Установите флажки **Использовать маску** рядом с полями **Тип контроллера (PID)** и **Серийный номер**, если вы хотите, чтобы выбранное правило разрешало подключение всех внешних устройств с указанными данными о производителе устройства, а также типе контроллера и серийном номере устройства.

   Если хотя бы в одном поле установлен флажок **Использовать маску**, данные в полях, в которых установлен этот флажок, заменяются символом * и не учитываются при применении правила.
5. Если требуется, введите дополнительную информацию о правиле в поле **Комментарий**. Например, уточните, на какие устройства должно распространяться правило.
6. Нажмите на кнопку **ОК**.

Настроенные параметры правила будут сохранены. Область применения правила будет расширена в соответствии с указанной маской пути к экземпляру устройства.

Настройка задачи Формирование правил контроля устройств

Чтобы настроить задачу Формирование правил контроля устройств, выполните следующие действия:

1. В дереве Консоли программы разверните узел **Автоматическое формирование правил**.
2. Выберите вложенный узел **Формирование правил контроля устройств**.
3. В панели результатов узла **Формирование правил контроля устройств** перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи**.
4. На закладке **Общие** в блоке **Режим генерации** выберите режим работы задачи:
   - **Учитывать данные системы обо всех когда-либо подключавшихся устройствах**
   - **Учитывать данные только об устройствах, подключенных в текущий момент**
5. В разделе **По завершении задачи** укажите действия, которые программа Kaspersky Embedded Systems Security должна выполнять по завершении задачи:

- **Добавлять разрешающие правила в список правил контроля устройств**
- **Принцип добавления**
- **Экспортировать разрешающие правила в файл**
- **Добавлять информацию о сервере в имя файла**

6. На закладках **Расписание** и **Дополнительно** настройте расписание запуска задачи.
7. В окне **Параметры задачи** нажмите на кнопку **OK**.

Kaspersky Embedded Systems Security немедленно применит новые значения параметров в выполняющейся задаче. Данные о дате и времени изменения параметров, а также значения параметров задачи до и после изменения будут сохранены в журнале системного аудита.

Управление Контролем устройств с помощью Веб-плагина Консоли программы-

В этом разделе описана навигация в интерфейсе Веб-плагина и настройка параметров задачи на защищаемом устройстве.

1. В главном окне веб-консоли выберите **Устройства** → **Политики и профили**.
2. Выберите политику, которую вы хотите настроить.
3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.
4. Выберите раздел **Контроль активности на компьютерах**.
5. Нажмите на кнопку **Параметры** в подразделе **Контроль устройств**.
6. Настройте параметры, приведены в следующей таблице.

Параметры задачи Контроль устройств

Параметр	Описание
Активный	Kaspersky Embedded Systems Security контролирует с помощью правил подключение съемных дисков и других внешних устройств и запрещает или разрешает использование всех устройств в соответствии с принципом запрета по умолчанию и заданными разрешающими правилами. Использование доверенных внешних устройств разрешено. Использование недоверенных внешних устройств запрещено по умолчанию.
Только статистика	Kaspersky Embedded Systems Security не контролирует подключение съемных дисков и других внешних устройств, а только фиксирует в журнале выполнения задачи информацию о подключениях и регистрации внешних устройств на защищаемом устройстве, а также о разрешающих правилах контроля устройств, сработавших при подключении устройств. Использование всех внешних устройств разрешено. Этот режим установлен по умолчанию.
Разрешать все внешние устройства, если задача Контроль	Флажок разрешает или запрещает использование внешних устройств, если задача Контроль устройств не выполняется. Если флажок установлен и задача Контроль устройств не выполняется, Kaspersky Embedded Systems Security разрешает использовать любые внешние устройства на защищаемом устройстве.

устройств не выполняется	Если флажок снят, программа запрещает использовать недоверенные внешние устройства на защищаемом устройстве в следующих случаях: если не выполняется задача Контроль устройств или если остановлена служба Kaspersky Security. Рекомендуется использовать этот вариант для обеспечения максимальной защиты от угроз компьютерной безопасности, возникающих при файловом обмене с внешними устройствами. По умолчанию флажок снят.
Правила контроля устройств	Можно настраивать список правил контроля устройств.
Управление задачами	Вы можете настроить расписание запуска задачи.

Управление сетевым экраном

Этот раздел содержит информацию о задаче Управление сетевым экраном и инструкции о том, как настроить параметры этой задачи.

О задаче Управление сетевым экраном

Kaspersky Embedded Systems Security обеспечивает надежное и удобное решение для защиты сетевых подключений с помощью задачи Управление сетевым экраном.

Задача Управление сетевым экраном не выполняет самостоятельную фильтрацию сетевого трафика, но предоставляет возможность управления брандмауэром Windows с помощью графического интерфейса Kaspersky Embedded Systems Security. В ходе выполнения задачи Управление сетевым экраном Kaspersky Embedded Systems Security полностью принимает на себя управление параметрами и политиками сетевого экрана операционной системы и блокирует любую возможность настройки сетевого экрана другими способами.

В ходе установки программы компонент Управление сетевым экраном считывает и копирует состояние брандмауэра Windows, а также все заданные правила. В дальнейшем изменение набора правил или их параметров, а также остановка или запуск сетевого экрана возможны только через Kaspersky Embedded Systems Security.

Если при установке Kaspersky Embedded Systems Security брандмауэр Windows выключен, задача Управление сетевым экраном не выполняется по завершении установки. Если при установке программы брандмауэр Windows включен, задача Управление сетевым экраном выполняется по завершении установки и блокирует все сетевые подключения, не разрешенные заданными правилами.

Компонент Управление сетевым экраном не входит в набор компонентов рекомендуемой установки и не устанавливается по умолчанию.

Задача Управление сетевым экраном форсирует блокирование всех входящих и исходящих подключений, если они не разрешены заданными правилами задачи.

Задача регулярно опрашивает брандмауэр Windows и контролирует его состояние. По умолчанию интервал опроса составляет 1 минуту и не может быть изменен. Если Kaspersky Embedded Systems Security обнаруживает несовпадение параметров брандмауэра Windows и параметров задачи Управление сетевым экраном, программа принудительно применяет параметры задачи в брандмауэре Windows.

Опрос брандмауэра Windows происходит каждую минуту, что позволяет Kaspersky Embedded Systems Security контролировать следующие данные:

- статус работы брандмауэра Windows;
- статус правил, добавленных другими программами или инструментами (например, добавление нового правила программы для порта или программы с помощью wf.msc) после установки Kaspersky Embedded Systems Security.

После передачи правил брандмауэру Windows, Kaspersky Embedded Systems Security создает набор правил Kaspersky Security Group в оснастке Брандмауэр Windows. Этот набор содержит все правила, созданные программой Kaspersky Embedded Systems Security с помощью задачи Управление сетевым экраном. Правила, входящие в набор Kaspersky Security Group, не контролируются программой при опросе и не синхронизируются автоматически со списком правил, заданным в параметрах задачи Управление сетевым экраном.

Чтобы обновить список правил Kaspersky Security Group вручную,

перезапустите задачу Управление сетевым экраном Kaspersky Embedded Systems Security.

Вы также можете изменять правила Kaspersky Security Group вручную через оснастку Брандмауэр Windows.

Запуск задачи Управление сетевым экраном невозможен, если брандмауэр Windows находится под управлением групповой политики Kaspersky Security Center.

О правилах сетевого экрана

Задача Управление сетевым экраном контролирует фильтрацию входящего и исходящего трафика с помощью разрешающих правил, которые принудительно применяются в брандмауэре Windows при выполнении задачи.

При первом запуске задачи Kaspersky Embedded Systems Security считывает и копирует все разрешающие правила для входящего трафика, заданные в параметрах брандмауэра Windows, в параметры задачи Управление сетевым экраном. При дальнейшей работе программа действует в соответствии со следующими алгоритмами:

- Если в параметрах брандмауэра Windows создается новое правило (вручную или автоматически при установке новой программы), Kaspersky Embedded Systems Security удаляет такое правило.
- Если в параметрах брандмауэра Windows удаляется существующее правило, Kaspersky Embedded Systems Security восстанавливает это правило при повторном запуске задачи.
- Если в параметрах брандмауэра Windows изменяются параметры существующего правила, Kaspersky Embedded Systems Security отменяет изменения.
- Если в параметрах задачи Управление сетевым экраном создается новое правило, Kaspersky Embedded Systems Security принудительно применяет это правило в брандмауэре Windows.
- Если в параметрах задачи Управление сетевым экраном удаляется существующее правило, Kaspersky Embedded Systems Security принудительно удаляет это правило из параметров брандмауэра Windows.

Kaspersky Embedded Systems Security не работает с запрещающими правилами, а также с правилами, контролирующими исходящий трафик. В момент запуска задачи Управление сетевым экраном Kaspersky Embedded Systems Security удаляет все правила этих типов в параметрах брандмауэра Windows.

Вы можете задавать, удалять и редактировать правила для фильтрации входящего трафика.

Вы не можете задать новое правило для контроля исходящего трафика через параметры задачи Управление сетевым экраном. Все правила сетевого экрана, заданные через Kaspersky Embedded Systems Security, контролируют только входящий трафик.

Можно управлять различными типами правил сетевого экрана: для программ и для портов.

Правила для приложений

Правила этого типа выборочно разрешают сетевые подключения для указанных приложений. Критерием срабатывания таких правил является путь к исполняемому файлу.

Вы можете управлять правилами для приложений:

- добавлять новые правила;
- удалять существующие правила;
- активировать или деактивировать заданные правила;
- изменять параметры заданных правил: указывать имя правила, путь к исполняемому файлу и область применения правила.

Правила для портов

Правила этого типа разрешают сетевые подключения для указанных портов и протоколов (TCP / UDP). Критериями срабатывания таких правил являются номер порта и тип протокола.

Вы можете управлять правилами для портов:

- добавлять новые правила;
- удалять существующие правила;
- активировать или деактивировать заданные правила;
- изменять параметры заданных правил: указывать имя правила, номер порта, тип протокола и область применения правила.

Правила для портов предполагают более широкую область действия, чем правила для приложений. Разрешая подключения с помощью правил для портов, вы снижаете уровень безопасности защищаемого устройства.

Параметры по умолчанию для задачи Управление сетевым экраном

По умолчанию в задаче Управление сетевым экраном используются параметры, описанные в таблице ниже. Вы можете изменять значения этих параметров.

Параметры по умолчанию для задачи Управление сетевым экраном

Параметр	Значение по умолчанию	Описание
Правила сетевого экрана для программы	Включено два заданных по умолчанию правила для программы.	Можно выключить заданные по умолчанию правила и добавлять новые правила.
Правила сетевого экрана для портов	Включено шесть заданных по умолчанию правил для портов.	Можно выключить заданные по умолчанию правила и добавлять новые правила.
Расписание запуска задачи	Время первого запуска не задано.	Задача Управление сетевым экраном не запускается автоматически при запуске программы Kaspersky Embedded Systems Security. Вы можете настроить запуск задачи по расписанию.

Управление правилами сетевого экрана с помощью Плагина управления

В этом разделе описано управление правилами сетевого экрана с помощью интерфейса Плагина управления.

Включение и выключение правил сетевого экрана

Чтобы включить или выключить существующее правило фильтрации входящего трафика, выполните следующие действия:

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить параметры программы.
3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
   - Чтобы настроить параметры программы для группы защищаемых устройств, выберите закладку **Политики** и откройте окно **Свойства: <Имя политики>**.
   - Чтобы настроить параметры программы для отдельного защищаемого устройства, выберите закладку **Устройства** и откройте окно **Параметры программы**.

     Если к устройству применяется активная политика Kaspersky Security Center, запрещающая изменение параметров программы, эти параметры недоступны для изменения в окне **Параметры программы**.
4. В разделе **Контроль активности в сети** нажмите на кнопку **Настройка** в подразделе **Управление сетевым экраном**.
5. В открывшемся окне нажмите на кнопку **Список правил**.

   Откроется окно **Правила сетевого экрана**.
6. В зависимости от типа правила, статус которого вы хотите изменить, выберите закладку **Приложения** или **Порты**.

7. В списке правил найдите правило, статус которого вы хотите изменить, и выполните одно из следующих действий:

   - Если вы хотите, чтобы неактивное правило применялось, установите флажок слева от имени правила.

     Выбранное правило будет активировано.

   - Если вы хотите, чтобы активное правило не применялось, снимите флажок слева от имени правила.

     Выбранное правило будет выключено.

8. В окне **Правила сетевого экрана** нажмите на кнопку **OK**.

9. В окне **Управление сетевым экраном** нажмите на кнопку **OK**.

10. В окне **Свойства: <Имя политики>** нажмите на кнопку **OK**.

Настроенные изменения параметров задачи будут сохранены. Новые параметры правил будут отправлены в брандмауэр Windows.

Добавление правил сетевого экрана вручную

Вы можете добавлять и редактировать только правила для приложений и портов. Вы не можете добавлять новые или редактировать существующие правила для групп.

Чтобы добавить новое или изменить существующее правило фильтрации входящего трафика, выполните следующие действия:

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.

2. Выберите группу администрирования, для которой требуется настроить параметры программы.

3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:

   - Чтобы настроить параметры программы для группы защищаемых устройств, выберите закладку **Политики** и откройте окно **Свойства: <Имя политики>**.

   - Чтобы настроить параметры программы для отдельного защищаемого устройства, выберите закладку **Устройства** и откройте окно **Параметры программы**.

     Если к устройству применяется активная политика Kaspersky Security Center, запрещающая изменение параметров программы, эти параметры недоступны для изменения в окне **Параметры программы**.

4. В разделе **Контроль активности в сети** нажмите на кнопку **Настройка** в подразделе **Управление сетевым экраном**.

5. В открывшемся окне нажмите на кнопку **Список правил**.

   Откроется окно **Правила сетевого экрана**.

6. В зависимости от типа правила, которое вы хотите добавить, выберите закладку **Приложения** или **Порты** и выполните одно из следующих действий:

- Чтобы изменить существующее правило, в списке правил выберите требуемое правило и нажмите на кнопку **Изменить**.
- Чтобы создать новое правило, нажмите на кнопку **Добавить**.

  В зависимости от типа настраиваемого правила, откроется окно **Настроить правило для приложения** или **Настроить правило для порта**.

7. В открывшемся окне выполните следующие действия:

   - Если вы работаете с правилом для приложения, выполните следующие действия:

     a. В поле **Имя правила** введите название правила.

     b. В поле **Путь к приложению** укажите путь к исполняемому файлу программы, подключения для которого вы хотите разрешить с помощью настраиваемого правила.

     Вы можете задать путь вручную или с помощью кнопки **Обзор**.

     c. В поле **Область применения правила** укажите сетевые адреса, к которым будет применено настраиваемое правило.

     Для IP-адресов поддерживается только формат IPv4.

   - Если вы работаете с правилом для порта, выполните следующие действия:

     a. В поле **Имя правила** введите название правила.

     b. В поле **Номер порта** укажите номер порта, для которого программа будет разрешать соединения.

     c. Выберите тип протокола (TCP / UDP), для которого программа будет разрешать соединения.

     d. В поле **Область применения правила** укажите сетевые адреса, к которым будет применено настраиваемое правило.

     Для IP-адресов поддерживается только формат IPv4.

8. В окне **Настроить правило для приложения** или **Настроить правило для порта** нажмите на кнопку **OK**.
9. В окне **Управление сетевым экраном** нажмите на кнопку **OK**.
10. В окне **Свойства: <Имя политики>** нажмите на кнопку **OK**.

Настроенные изменения параметров задачи будут сохранены. Новые параметры правил будут отправлены в брандмауэр Windows.

Удаление правил сетевого экрана

Вы можете удалять только правила для приложений и портов. Вы не можете удалять существующие правила для групп.

Чтобы удалить существующее правило фильтрации входящего трафика, выполните следующие действия:

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить параметры программы.
3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
   - Чтобы настроить параметры программы для группы защищаемых устройств, выберите закладку **Политики** и откройте окно **Свойства: <Имя политики>**.
   - Чтобы настроить параметры программы для отдельного защищаемого устройства, выберите закладку **Устройства** и откройте окно **Параметры программы**.

     Если к устройству применяется активная политика Kaspersky Security Center, запрещающая изменение параметров программы, эти параметры недоступны для изменения в окне **Параметры программы**.
4. В разделе **Контроль активности в сети** нажмите на кнопку **Настройка** в подразделе **Управление сетевым экраном**.
5. В открывшемся окне нажмите на кнопку **Список правил**.

   Откроется окно **Правила сетевого экрана**.
6. В зависимости от типа правила, статус которого вы хотите изменить, выберите закладку **Приложения** или **Порты**.
7. В списке правил выберите правило, которое вы хотите удалить.
8. Нажмите на кнопку **Удалить**.

   Выбранное правило будет удалено.
9. В окне **Правила сетевого экрана** нажмите на кнопку **ОК**.
10. В окне **Управление сетевым экраном** нажмите на кнопку **ОК**.
11. В окне **Свойства: <Имя политики>** нажмите на кнопку **ОК**.

Настроенные изменения параметров задачи Управление сетевым экраном будут сохранены. Новые параметры правил будут отправлены в брандмауэр Windows.

Управление правилами сетевого экрана с помощью Консоли программы

В этом разделе описано управление правилами сетевого экрана с помощью Консоли программы.

Включение и выключение правил сетевого экрана

Чтобы включить или выключить существующее правило фильтрации входящего трафика, выполните следующие действия:

1. В дереве Консоли программы разверните узел **Контроль компьютера**.

2. Выберите вложенный узел **Управление сетевым экраном**.

3. В панели результатов узла **Правила сетевого экрана** перейдите по ссылке **Управление сетевым экраном**.

   Откроется окно **Правила сетевого экрана**.

4. В зависимости от типа правила, статус которого вы хотите изменить, выберите закладку **Приложения** или **Порты**.

5. В списке правил найдите правило, статус которого вы хотите изменить, и выполните одно из следующих действий:

   - Если вы хотите, чтобы неактивное правило применялось, установите флажок слева от имени правила.

     Выбранное правило будет активировано.

   - Если вы хотите, чтобы активное правило не применялось, снимите флажок слева от имени правила.

     Выбранное правило будет выключено.

6. В окне **Правила сетевого экрана** нажмите на кнопку **Сохранить**.

Настроенные изменения параметров задачи будут сохранены. Новые параметры правил будут отправлены в брандмауэр Windows.

Добавление правил сетевого экрана вручную

Чтобы добавить новое или изменить существующее правило фильтрации входящего трафика, выполните следующие действия:

1. В дереве Консоли программы разверните узел **Контроль компьютера**.

2. Выберите вложенный узел **Управление сетевым экраном**.

3. В панели результатов узла **Правила сетевого экрана** перейдите по ссылке **Управление сетевым экраном**.

   Откроется окно **Правила сетевого экрана**.

4. В зависимости от типа правила, которое вы хотите добавить, выберите закладку **Приложения** или **Порты** и выполните одно из следующих действий:

   - Чтобы изменить существующее правило, в списке правил выберите требуемое правило и нажмите на кнопку **Изменить**.

   - Чтобы создать новое правило, нажмите на кнопку **Добавить**.

     В зависимости от типа настраиваемого правила, откроется окно **Настроить правило для приложения** или **Настроить правило для порта**.

5. В открывшемся окне выполните следующие действия:

   - Если вы работаете с правилом для приложения, выполните следующие действия:

     a. В поле **Имя правила** введите название правила.

b. В поле **Путь к приложению** укажите путь к исполняемому файлу программы, подключения для которого вы хотите разрешить с помощью настраиваемого правила.

Вы можете задать путь вручную или с помощью кнопки **Обзор**.

c. В поле **Область применения правила** укажите сетевые адреса, к которым будет применено настраиваемое правило.

Для IP-адресов поддерживается только формат IPv4.

- Если вы работаете с правилом для порта, выполните следующие действия:

a. В поле **Имя правила** введите название правила.

b. В поле **Номер порта** укажите номер порта, для которого программа будет разрешать соединения.

c. Выберите тип протокола (TCP / UDP), для которого программа будет разрешать соединения.

d. В поле **Область применения правила** укажите сетевые адреса, к которым будет применено настраиваемое правило.

Для IP-адресов поддерживается только формат IPv4.

6. В окне **Настроить правило для приложения** или **Настроить правило для порта** нажмите на кнопку **OK**.

7. В окне **Правила сетевого экрана** нажмите на кнопку **Сохранить**.

Настроенные изменения параметров задачи будут сохранены. Новые параметры правил будут отправлены в брандмауэр Windows.

Удаление правил сетевого экрана

Вы можете удалять только правила для приложений и портов. Вы не можете удалять существующие правила для групп.

Чтобы удалить существующее правило фильтрации входящего трафика, выполните следующие действия:

1. В дереве Консоли программы разверните узел **Контроль компьютера**.

2. Выберите вложенный узел **Управление сетевым экраном**.

3. В панели результатов узла **Правила сетевого экрана** перейдите по ссылке **Управление сетевым экраном**.

Откроется окно **Правила сетевого экрана**.

4. В зависимости от типа правила, статус которого вы хотите изменить, выберите закладку **Приложения** или **Порты**.

5. В списке правил выберите правило, которое вы хотите удалить.

6. Нажмите на кнопку **Удалить**.

Выбранное правило будет удалено.

7. В окне **Правила сетевого экрана** нажмите на кнопку **Сохранить**.

Настроенные изменения параметров задачи будут сохранены. Новые параметры правил будут отправлены в брандмауэр Windows.

Управление правилами сетевого экрана с помощью Веб-плагина

Чтобы настроить правила сетевого экрана с помощью Веб-плагина, выполните следующие действия:

1. В главном окне веб-консоли выберите **Устройства** → **Политики и профили**.
2. Выберите политику, которую вы хотите настроить.
3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.
4. Выберите раздел **Контроль активности в сети**.
5. Нажмите на кнопку **Параметры** в подразделе **Управление сетевым экраном**.
6. Настройте параметры, приведены в следующей таблице.

Параметры задачи Управление сетевым экраном

Параметр	Описание
Применять пользовательские правила для анализа журналов	Пользовательские правила можно включать, отключать, добавлять или изменять. Этот параметр доступен в таблице со списком пользовательских правил.
Использовать предзаданные правила для анализа журналов	Можно включить или выключить эвристический анализатор, отвечающий за обнаружение аномальной активности на защищаемом устройстве. Этот параметр доступен в таблице со списком пользовательских правил.
Обработка попытки подбора пароля, если неправильный пароль вводится с заданной частотой	Можно указать количество попыток и промежуток времени, в течение которого выполнялись попытки, в качестве критерия срабатывания эвристического анализатора.
Обработка сетевого входа, если обнаружена попытка входа в течение заданного промежутка времени	Можно указать начало и конец временного интервала, в течение которого при выполнении попытки входа Kaspersky Embedded Systems Security расценивает данное действие как аномальную активность.
Исключение пользователей	Можно указать пользователей, которые не будут являться критериями срабатывания эвристического анализатора.
Исключение IP-адресов	Можно указать IP-адреса, которые не будут являться критериями срабатывания эвристического анализатора.
Управление задачами	Вы можете настроить расписание запуска задачи.

Включение и выключение правил сетевого экрана

Чтобы включить или выключить существующее правило фильтрации входящего трафика, выполните следующие действия:

1. В главном окне веб-консоли выберите **Устройства** → **Политики и профили**.
2. Выберите политику, которую вы хотите настроить.
3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.
4. Выберите раздел **Контроль активности в сети**.
5. Нажмите на кнопку **Параметры** в подразделе **Управление сетевым экраном**.
6. В зависимости от типа правила, статус которого вы хотите изменить, выберите закладку **Настроить правило для приложения** или **Настроить правило для порта**.
7. В списке правил найдите правило, статус которого вы хотите изменить, и выполните одно из следующих действий:
   - Если вы хотите, чтобы неактивное правило применялось, включите переключатель слева от имени правила.
   - Если вы хотите, чтобы активное правило не применялось, выключите переключатель слева от имени правила.
8. Нажмите на кнопку **OK**.

Настроенные изменения параметров задачи будут сохранены. Новые параметры правил будут отправлены в брандмауэр Windows.

Добавление правил сетевого экрана вручную

Чтобы добавить новое или изменить существующее правило фильтрации входящего трафика, выполните следующие действия:

1. В главном окне веб-консоли выберите **Устройства** → **Политики и профили**.
2. Выберите политику, которую вы хотите настроить.
3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.
4. Выберите раздел **Контроль активности в сети**.
5. Нажмите на кнопку **Параметры** в подразделе **Управление сетевым экраном**.
6. В зависимости от типа правила, статус которого вы хотите изменить, выберите закладку **Настроить правило для приложения** или **Настроить правило для порта** и выполните одно из следующих действий:
   - Чтобы изменить существующее правило, выберите требуемое правило и нажмите на кнопку **Изменить**.

- Чтобы создать новое правило, нажмите на кнопку **Добавить**.

7. В правой части окна выполните следующие действия:

   - Если вы работаете с правилом для приложения, выполните следующие действия:

     a. В поле **Имя правила** введите название правила.

     b. В поле **Путь к приложению** укажите путь к исполняемому файлу программы, подключения для которого вы хотите разрешить с помощью настраиваемого правила.

     c. В поле **Область применения правила** укажите сетевые адреса, к которым будет применено настраиваемое правило.

     Для IP-адресов поддерживается только формат IPv4.

   - Если вы работаете с правилом для порта, выполните следующие действия:

     a. В поле **Имя правила** введите название правила.

     b. Укажите номер порта, для которого программа будет разрешать соединения.

     c. Выберите тип протокола (TCP / UDP), для которого программа будет разрешать соединения.

     d. В поле **Область применения правила** укажите сетевые адреса, к которым будет применено настраиваемое правило.

     Для IP-адресов поддерживается только формат IPv4.

8. Нажмите на кнопку **OK**.

9. В окне **Управление сетевым экраном** нажмите на кнопку **OK**.

Настроенные изменения параметров задачи будут сохранены. Новые параметры правил будут отправлены в брандмауэр Windows.

Удаление правил сетевого экрана

Вы можете удалять только правила для приложений и портов. Вы не можете удалять существующие правила для групп.

Чтобы удалить существующее правило фильтрации входящего трафика, выполните следующие действия:

1. В главном окне веб-консоли выберите **Устройства** → **Политики и профили**.

2. Выберите политику, которую вы хотите настроить.

3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.

4. Выберите раздел **Контроль активности в сети**.

5. Нажмите на кнопку **Параметры** в подразделе **Управление сетевым экраном**.

6. В зависимости от типа правила, которое вы хотите удалить, выберите закладку **Настроить правило для приложения** или **Настроить правило для порта**.

7. В списке правил выберите правило, которое вы хотите удалить.

8. Нажмите на кнопку **Удалить**.

   Выбранное правило будет удалено.

9. Нажмите на кнопку **ОК**.

Настроенные изменения параметров задачи будут сохранены. Новые параметры правил будут отправлены в брандмауэр Windows.

Мониторинг файловых операций

Этот раздел содержит информацию о запуске и настройке задачи Мониторинг файловых операций.

О задаче Мониторинг файловых операций

Задача Мониторинг файловых операций предназначена для отслеживания действий, выполненных с указанными файлами или папками, в областях мониторинга, заданных в параметрах задачи. Вы можете использовать задачу, чтобы отслеживать изменения в файлах, которые могут указывать на нарушение безопасности на защищаемом устройстве. Вы также можете настроить отслеживание изменений файлов в периоды обрыва мониторинга.

Обрыв мониторинга – это период, когда область мониторинга временно выпадает из поля действия задачи, например, из-за приостановки выполнения задачи или из-за физического отсутствия внешнего устройства на защищаемом устройстве. Kaspersky Embedded Systems Security сообщит об обнаружении файловых операций в области мониторинга, как только внешнее устройство будет вновь подключено.

Приостановка выполнения задачи в заданной области мониторинга, вызванная переустановкой компонента Мониторинг файловых операций, не является обрывом мониторинга. В этом случае задача Мониторинг файловых операций не выполняется.

Требования к среде

Для запуска задачи Мониторинг файловых операций должны выполняться следующие условия:

- На защищаемом устройстве установлено внешнее устройство, поддерживающее файловую систему ReFS или NTFS.
- USN-журнал Windows должен быть включен. На основе опроса USN-журнала компонент получает данные о файловых операциях.

  Если вы включили USN-журнал после того, как было создано правило для тома и запущена задача Мониторинг файловых операций, необходимо перезапустить задачу. В противном случае, данное правило не будет учитываться при мониторинге.

Исключения для области мониторинга

Вы можете создать исключения из области мониторинга. Исключения задаются для каждого отдельного правила и работают только для указанной области мониторинга. Вы можете задать неограниченное количество исключений для каждого правила.

Исключения имеют более высокий приоритет, чем область мониторинга, и не контролируются задачей, даже если указанная папка или файл входят в область мониторинга. Если в параметрах одного из правил задана область мониторинга, которая является нижнеуровневой по отношению к папке, заданной в исключениях, такая область мониторинга не будет учитываться при выполнении задачи.

Для задания исключений вы можете использовать те же маски, что и для задания областей мониторинга.

О правилах мониторинга файловых операций

Задача Мониторинг файловых операций выполняется на основе правил мониторинга файловых операций. Вы можете настраивать условия срабатывания правила и регулировать уровень важности событий для обнаруженных файловых операций, регистрируемых в журнале выполнения задачи, с помощью критериев срабатывания правила.

Правило мониторинга файловых операций задается для каждой указанной области мониторинга.

Вы можете настраивать следующие критерии срабатывания правил:

- доверенные пользователи;
- маркеры файловых операций.

Доверенные пользователи

По умолчанию действия всех пользователей расцениваются программой как потенциальные нарушения безопасности. Список доверенных пользователей пуст. Вы можете настраивать уровни важности события, формируя список доверенных пользователей в параметрах правила мониторинга файловых операций.

Недоверенный пользователь – любой пользователь, не указанный в списке доверенных в параметрах правила области мониторинга. Если Kaspersky Embedded Systems Security обнаруживает файловую операцию, выполненную недоверенным пользователем, задача Мониторинг файловых операций фиксирует Критическое событие в журнале выполнения задачи.

Доверенный пользователь – пользователь или группа пользователей, которым разрешено выполнение файловых операций в указанной области мониторинга. Если Kaspersky Embedded Systems Security обнаруживает файловую операцию, выполненную доверенным пользователем, задача Мониторинг файловых операций фиксирует Информационное событие в журнале выполнения задачи.

Kaspersky Embedded Systems Security не может определить пользователя, выполнившего операции в период обрыва мониторинга. В этом случае статус пользователя определяется как неизвестный.

Неизвестный пользователь – данный статус присваивается пользователю в случае, когда Kaspersky Embedded Systems Security не может получить данные о пользователе вследствие прерывания задачи или сбоя драйвера синхронизации данных или USN-журнала. Если Kaspersky Embedded Systems Security обнаруживает файловую операцию, выполненную неизвестным пользователем, задача Мониторинг файловых операций фиксирует событие *Предупреждение* в журнале выполнения задачи.

Маркеры файловых операций

В ходе выполнения задачи Мониторинг файловых операций Kaspersky Embedded Systems Security определяет, что над файлом было произведено действие, с помощью маркеров файловых операций.

Маркер файловой операции – это единичный признак, которым может быть охарактеризована файловая операция.

Каждая файловая операция может представлять собой одно действие или цепочку действий с файлами. Каждое такое действие приравнивается к маркеру файловой операции. Если в цепочке файловой операции был обнаружен маркер, указанный вами в качестве критерия срабатывания правила мониторинга, программа зарегистрирует событие по факту совершения такой файловой операции.

Уровень важности фиксируемых событий не зависит от выбранных маркеров файловых операций или их количества.

По умолчанию Kaspersky Embedded Systems Security учитывает все доступные маркеры файловых операций. Вы можете выбрать маркеры файловых операций вручную в параметрах правил задачи (см. таблицу ниже).

Маркеры файловых операций

ID файловой операции	Маркер файловой операции	Поддерживаемые файловые системы
BASIC_INFO_CHANGE	изменены атрибуты или метки времени файла или папки	NTFS, ReFS
COMPRESSION_CHANGE	изменено сжатие файла или папки	NTFS, ReFS
DATA_EXTEND	размер файла или папки увеличен	NTFS, ReFS
DATA_OVERWRITE	перезаписаны данные в файле или папке	NTFS, ReFS
DATA_TRUNCATION	файл или папка усечены	NTFS, ReFS
EA_CHANGE	изменены расширенные атрибуты файла или папки	только NTFS
ENCRYPTION_CHANGE	изменен статус шифрования файла или папки	NTFS, ReFS
FILE_CREATE	файл или папка созданы впервые	NTFS, ReFS
FILE_DELETE	Файл или папка удалены, минуя корзину, с помощью команды SHIFT+DEL	NTFS, ReFS
HARD_LINK_CHANGE	жесткая связь создана или удалена для файла или папки	только NTFS
INDEXABLE_CHANGE	изменен статус индексирования файла или папки	NTFS, ReFS
INTEGRITY_CHANGE	изменен атрибут целостности для именованного файлового потока	только ReFS
NAMED_DATA_EXTEND	размер именованного файлового потока увеличен	NTFS, ReFS
NAMED_DATA_OVERWRITE	именованный файловый поток перезаписан	NTFS, ReFS
NAMED_DATA_TRUNCATION	именованный файловый поток усечен	NTFS, ReFS
OBJECT_ID_CHANGE	изменен идентификатор файла или папки	NTFS, ReFS
RENAME_NEW_NAME	присвоено новое имя для файла или папки	NTFS, ReFS
REPARSE_POINT_CHANGE	создана новая или изменена существующая точка повторного анализа для файла или папки	NTFS, ReFS
SECURITY_CHANGE	изменены права доступа к файлу или папке	NTFS, ReFS
STREAM_CHANGE	создан новый или изменен существующий именованный файловый поток	NTFS, ReFS
TRANSACTED_CHANGE	именованный файловый поток изменен транзакцией TxF	только ReFS

Параметры по умолчанию для задачи Мониторинг файловых операций

По умолчанию в задаче Мониторинг файловых операций используются параметры, описанные в таблице ниже. Вы можете изменять значения этих параметров.

Параметры по умолчанию для задачи Мониторинг файловых операций

Параметр	Значение по умолчанию	Описание
Область мониторинга	Не задано	Вы можете задать папки и файлы, действия над которыми будут отслеживаться. Для папок и файлов заданной области мониторинга будут формироваться события мониторинга.
Список **Пользователи**	Не задано	Вы можете задать пользователей и группы пользователей, действия которых в указанных папках будут расцениваться компонентом как безопасные.
Фиксировать события о файловых операциях, выполненных в период обрыва мониторинга	Применяется	Вы можете включать или выключать учет файловых операций, которые были выполнены в указанных областях мониторинга в период простоя задачи.
Блокировать попытки компрометации журнала USN	Применяется	Вы можете включать и выключать защиту USN-журнала.
Учитывать исключенные области контроля	Не применяется	Вы можете контролировать применение исключений для папок, где не требуется выполнять контроль за файловыми операциями. При выполнении задачи Мониторинг файловых операций Kaspersky Embedded Systems Security пропускает области мониторинга, заданные в качестве исключений.
Контрольная сумма	Не применяется	Вы можете настроить расчет контрольной суммы файла после произведенных в нем изменений.
Маркеры файловых операций	Учитываются все доступные маркеры файловых операций	Вы можете задать набор маркеров файловых операций. Если файловая операция, выполненная в области мониторинга, характеризуется хотя бы одним из указанных маркеров, Kaspersky Embedded Systems Security формирует событие аудита.
Расписание запуска задачи	Время первого запуска не задано.	Вы можете настроить расписание запуска задачи.

Управление мониторингом файловых операций с помощью Плагина управления

В этом разделе описана настройка параметров задачи Мониторинг файловых операций с помощью Плагина управления.

Настройка задачи Мониторинг файловых операций

Чтобы настроить общие параметры задачи Мониторинг файловых операций, выполните следующие действия:

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.

2. Выберите группу администрирования, для которой требуется настроить параметры программы.

3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:

   - Чтобы настроить параметры программы для группы защищаемых устройств, выберите закладку **Политики** и откройте окно **Свойства: <Имя политики>**.

   - Чтобы настроить параметры программы для отдельного защищаемого устройства, выберите закладку **Устройства** и откройте окно **Параметры программы**.

     Если к устройству применяется активная политика Kaspersky Security Center, запрещающая изменение параметров программы, эти параметры недоступны для изменения в окне **Параметры программы**.

4. В разделе **Диагностика системы** в подразделе **Мониторинг файловых операций** нажмите на кнопку **Настройка**.

   Откроется окно **Мониторинг файловых операций**.

5. В открывшемся окне на закладке **Параметры мониторинга файловых операций** настройте следующие параметры:

   a. Снимите или установите флажок **Фиксировать события о файловых операциях, выполненных в период обрыва мониторинга**.

   b. Снимите или установите флажок **Блокировать попытки компрометации журнала USN**.

      Этот флажок включает или выключает защиту USN-журнала.

      Если флажок установлен, Kaspersky Embedded Systems Security блокирует попытки удаления USN-журнала или компрометации содержимого USN-журнала.

      Если флажок снят, программа не контролирует изменения в USN-журнале.

      По умолчанию флажок установлен.

   c. Добавьте области мониторинга, которые будет контролировать задача.

6. На закладке **Управление задачей** настройте параметры запуска задачи по расписанию.

7. Нажмите на кнопку **OK**, чтобы сохранить изменения.

Настройка правил мониторинга

Чтобы добавить область мониторинга, выполните следующие действия:

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.

2. Выберите группу администрирования, для которой требуется настроить параметры программы.

3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:

   - Чтобы настроить параметры программы для группы защищаемых устройств, выберите закладку **Политики** и откройте окно **Свойства: <Имя политики>**.

   - Чтобы настроить параметры программы для отдельного защищаемого устройства, выберите закладку **Устройства** и откройте окно **Параметры программы**.

     Если к устройству применяется активная политика Kaspersky Security Center, запрещающая изменение параметров программы, эти параметры недоступны для изменения в окне **Параметры программы**.

4. В разделе **Диагностика системы** в подразделе **Мониторинг файловых операций** нажмите на кнопку **Настройка**.

   Откроется окно **Мониторинг файловых операций**.

5. В разделе **Область мониторинга** нажмите на кнопку **Добавить**.

   Откроется окно **Область мониторинга**.

6. Добавьте область мониторинга одним из следующих способов:

   - Если вы хотите выбрать папки через стандартный диалог Microsoft Windows:

     a. Нажмите на кнопку **Обзор**.

        Откроется стандартное окно Microsoft Windows **Обзор папок**.

     b. В открывшемся окне выберите папку, файловые операции в которой вы хотите контролировать, и нажмите на кнопку **OK**.

   - Если вы хотите задать область мониторинга вручную, добавьте путь с помощью одной из поддерживаемых масок:

     - <*.ext> – все файлы с расширением <ext>, независимо от их расположения;

     - <*\name.ext> – все файлы с именем <name> и расширением <ext>, независимо от их расположения;

     - <\dir*> – все файлы в папке <\dir>;

     - <\dir*\name.ext> – все файлы с именем <name> и расширением <ext> в папке <\dir> и всех ее подпапках.

   При задании области мониторинга вручную убедитесь, что путь соответствует формату: <буква тома>:\<маска>. Если том не указан, Kaspersky Embedded Systems Security не добавит указанную область мониторинга.

7. На закладке **Доверенные пользователи** нажмите на кнопку **Добавить**.

   Откроется стандартное окно Microsoft Windows **Выбор пользователей или групп**.

8. Выберите пользователей или группы пользователей, которым будут разрешены операции с файлами для выбранной области мониторинга, и нажмите на кнопку **OK**.

По умолчанию Kaspersky Embedded Systems Security считает недоверенными всех пользователей, не указанных в списке доверенных, и формирует для них события с уровнем важности Критический.

9. Выберите закладку **Маркеры файловых операций**.
10. Если требуется, выберите несколько маркеров, выполнив следующие действия:
    a. Выберите вариант **Обнаруживать файловые операции по следующим маркерам**.
    b. В списке доступных файловых операций установите флажки напротив тех операций, которые вы хотите контролировать.

По умолчанию Kaspersky Embedded Systems Security обнаруживает все маркеры файловых операций. Выбран вариант **Обнаруживать файловые операции по всем распознаваемым маркерам**.

11. Если вы хотите, чтобы программа Kaspersky Embedded Systems Security рассчитывала контрольную сумму файла после изменения, выполните следующие действия:
    a. Установите флажок **Рассчитывать контрольную сумму файла после файловой операции, если это возможно. Контрольная сумма будет указана в журнале выполнения задачи**.
    b. В раскрывающемся списке **Тип контрольной суммы** выберите один из следующих вариантов:
       - **Хеш MD5**
       - **Хеш SHA256**
12. Если вы хотите контролировать не все файловые операции, в списке доступных файловых операций установите флажки напротив операций, которые вы хотите контролировать.
13. Если требуется, добавьте исключения для области мониторинга, выполнив следующие действия:
    a. Выберите закладку **Исключения**.
    b. Установите флажок **Учитывать исключенные области контроля**.
    c. Нажмите на кнопку **Добавить**.
       Откроется окно **Выберите папку для добавления**.
    d. В открывшемся окне выберите папку, которую вы хотите исключить из области мониторинга.
    e. Нажмите на кнопку **OK**.
       Указанная папка добавится в список исключенных областей.
14. В окне **Область мониторинга** нажмите на кнопку **OK**.

Указанные параметры правил будут применяться к выбранной области мониторинга задачи Мониторинг файловых операций.

Управление мониторингом файловых операций с помощью Консоли программы

В этом разделе описана настройка параметров задачи Мониторинг файловых операций с помощью Консоли программы.

Настройка параметров задачи Мониторинг файловых операций

Чтобы настроить общие параметры задачи Мониторинг файловых операций, выполните следующие действия:

1. В дереве Консоли программы разверните узел **Диагностика системы**.
2. Выберите вложенный узел **Мониторинг файловых операций**.
3. В панели результатов узла **Мониторинг файловых операций** перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи**.
4. В открывшемся окне на закладке **Общие** настройте следующие параметры:

   a. Снимите или установите флажок **Фиксировать события о файловых операциях, выполненных в период обрыва мониторинга**.

   b. Снимите или установите флажок **Блокировать попытки компрометации журнала USN**.

   > Этот флажок включает или выключает защиту USN-журнала.
   >
   > Если флажок установлен, Kaspersky Embedded Systems Security блокирует попытки удаления USN-журнала или компрометации содержимого USN-журнала.
   >
   > Если флажок снят, программа не контролирует изменения в USN-журнале.
   >
   > По умолчанию флажок установлен.
5. На закладках **Расписание** и **Дополнительно** настройте расписание запуска задачи.
6. Нажмите на кнопку **OK**, чтобы сохранить изменения.

Настройка правил мониторинга

Чтобы добавить область мониторинга, выполните следующие действия:

1. В дереве Консоли программы разверните узел **Диагностика системы**.
2. Выберите вложенный узел **Мониторинг файловых операций**.
3. В панели результатов узла **Мониторинг файловых операций** перейдите по ссылке **Правила мониторинга файловых операций**.

Откроется окно **Мониторинг файловых операций**.

4. Добавьте область мониторинга одним из следующих способов:

   - Если вы хотите выбрать папки через стандартный диалог Microsoft Windows:

     a. В левой части окна нажмите на кнопку **Обзор**.

        Откроется стандартное окно Microsoft Windows **Обзор папок**.

     b. В открывшемся окне выберите папку, файловые операции в которой вы хотите контролировать, и нажмите на кнопку **OK**.

     c. Нажмите кнопку **Добавить**, чтобы программа Kaspersky Embedded Systems Security начала контролировать файловые операции в указанной области мониторинга.

   - Если вы хотите задать область мониторинга вручную, добавьте путь с помощью одной из поддерживаемых масок:

     - <*.ext> – все файлы с расширением <ext>, независимо от их расположения;
     - <*\name.ext> – все файлы с именем <name> и расширением <ext>, независимо от их расположения;
     - <\dir*> – все файлы в папке <\dir>;
     - <\dir*\name.ext> – все файлы с именем <name> и расширением <ext> в папке <\dir> и всех ее подпапках.

   При задании области мониторинга вручную убедитесь, что путь соответствует формату: <буква тома>:\<маска>. Если том не указан, Kaspersky Embedded Systems Security не добавит указанную область мониторинга.

   В правой части окна на закладке **Параметры правила** отобразятся доверенные пользователи и маркеры файловых операций, выбранные для этой области мониторинга.

5. В списке добавленных областей мониторинга выберите область, для которой хотите настроить другие параметры.

6. Выберите закладку **Пользователи**.

7. Нажмите на кнопку **Добавить**.

   Откроется стандартное окно Microsoft Windows **Выбор пользователей или групп**.

8. Выберите пользователей или группы пользователей, которые Kaspersky Embedded Systems Security будет считать доверенными для выбранной области мониторинга.

9. Нажмите на кнопку **OK**.

   По умолчанию Kaspersky Embedded Systems Security считает недоверенными всех пользователей, не указанных в списке доверенных, и формирует для них события с уровнем важности Критический.

10. Выберите закладку **Маркеры файловых операций**.

11. Если требуется, выберите несколько маркеров, выполнив следующие действия:

a. Выберите вариант **Обнаруживать файловые операции по следующим маркерам**.

b. В списке доступных файловых операций установите флажки напротив тех операций, которые вы хотите контролировать.

По умолчанию Kaspersky Embedded Systems Security обнаруживает все маркеры файловых операций. Выбран вариант **Обнаруживать файловые операции по всем распознаваемым маркерам**.

12. Если вы хотите, чтобы программа Kaspersky Embedded Systems Security рассчитывала контрольную сумму файла после изменения, выполните следующие действия:

a. В разделе **Контрольная сумма** установите флажок **Рассчитывать контрольную сумму измененного файла, если это возможно. Контрольная сумма будет указана в журнале выполнения задачи**.

b. В раскрывающемся списке **Рассчитывать контрольную сумму по алгоритму** выберите один из следующих вариантов:

- **Хеш MD5**
- **Хеш SHA256**

13. Если требуется, добавьте исключения для области мониторинга, выполнив следующие действия:

a. Выберите закладку **Исключения**.

b. Установите флажок **Учитывать исключенные области мониторинга**.

c. Нажмите на кнопку **Обзор**.

Откроется стандартное окно Microsoft Windows **Обзор папок**.

d. В открывшемся окне выберите папку, которую вы хотите исключить из области мониторинга.

e. Нажмите на кнопку **OK**.

f. Нажмите на кнопку **Добавить**.

Указанная папка добавится в список исключенных областей.

Вы также можете добавить исключения для области мониторинга вручную используя те же маски, что и для задания областей мониторинга.

14. Нажмите на кнопку **Сохранить**, чтобы применить новые параметры правил.

Управление мониторингом файловых операций с помощью Веб-плагина

В этом разделе описана настройка задачи Мониторинг файловых операций с помощью Веб-плагина.

Настройка задачи Мониторинг файловых операций

Чтобы настроить задачу Мониторинг файловых операций с помощью Веб-плагина, выполните следующие действия:

1. В главном окне веб-консоли выберите **Устройства** → **Политики и профили**.
2. Выберите политику, которую вы хотите настроить.
3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.
4. Выберите раздел **Диагностика системы**.
5. Нажмите на кнопку **Параметры** в подразделе **Мониторинг файловых операций**.
6. В открывшемся окне **Мониторинг файловых операций** на закладке **Параметры мониторинга файловых операций** настройте следующие параметры:
   a. Снимите или установите флажок **Фиксировать события о файловых операциях, выполненных в период обрыва мониторинга**.
   b. Снимите или установите флажок **Блокировать попытки компрометации журнала USN**.

   Этот флажок включает или выключает защиту USN-журнала.

   Если флажок установлен, Kaspersky Embedded Systems Security блокирует попытки удаления USN-журнала или компрометации содержимого USN-журнала.

   Если флажок снят, программа не контролирует изменения в USN-журнале.

   По умолчанию флажок установлен.
7. На закладке **Управление задачей** настройте расписание запуска задачи.
8. Нажмите на кнопку **ОК**, чтобы сохранить изменения.

Настройка правил мониторинга

Чтобы добавить область мониторинга, выполните следующие действия:

1. В главном окне веб-консоли выберите **Устройства** → **Политики и профили**.
2. Выберите политику, которую вы хотите настроить.
3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.
4. Выберите раздел **Диагностика системы**.
5. Нажмите на кнопку **Параметры** в подразделе **Мониторинг файловых операций**.
6. В открывшемся окне **Мониторинг файловых операций** перейдите на закладку **Параметры мониторинга файловых операций**.
7. В разделе **Журнал USN** нажмите на кнопку **Добавить**.

   Откроется окно **Область мониторинга**.

8. В разделе **Выполнять мониторинг файловых операций для областей** укажите путь с помощью поддерживаемой маски:

   - <*.ext> – все файлы с расширением <ext>, независимо от их расположения;
   - <*\name.ext> – все файлы с именем <name> и расширением <ext>, независимо от их расположения;
   - <\dir*> – все файлы в папке <\dir>;
   - <\dir*\name.ext> – все файлы с именем <name> и расширением <ext> в папке <\dir> и всех ее подпапках.

   При задании области мониторинга вручную убедитесь, что путь соответствует формату: <буква тома>:\<маска>. Если том не указан, Kaspersky Embedded Systems Security не добавит указанную область мониторинга.

9. На закладке **Доверенные пользователи** нажмите на кнопку **Добавить**.

   В поле **Имя пользователя** укажите пользователя.

   По умолчанию Kaspersky Embedded Systems Security считает недоверенными всех пользователей, не указанных в списке доверенных, и формирует для них события с уровнем важности Критический.

10. Выберите закладку **Маркеры файловых операций**.

11. Если требуется, выберите несколько маркеров, выполнив следующие действия:

    a. Выберите вариант **Обнаруживать файловые операции по следующим маркерам**.

    b. В списке доступных файловых операций установите флажки напротив тех операций, которые вы хотите контролировать.

    По умолчанию Kaspersky Embedded Systems Security обнаруживает все маркеры файловых операций. Выбран вариант **Обнаруживать файловые операции по всем распознаваемым маркерам**.

12. Если вы хотите, чтобы программа Kaspersky Embedded Systems Security рассчитывала контрольную сумму файла после изменения, выполните следующие действия:

    a. Установите флажок **Рассчитывать контрольную сумму файла после файловой операции, если это возможно. Контрольная сумма будет указана в журнале выполнения задачи**.

    b. В раскрывающемся списке **Тип контрольной суммы** выберите один из следующих вариантов:

       - **Хеш SHA256**
       - **Хеш MD5**

13. Если вы хотите контролировать не все файловые операции, в списке доступных файловых операций установите флажки напротив операций, которые вы хотите контролировать.

14. Если требуется, добавьте исключения для области мониторинга, выполнив следующие действия:

    a. Выберите закладку **Исключения**.

b. Установите флажок **Учитывать исключенные области контроля**.

c. Нажмите на кнопку **Добавить**.

Откроется окно **Выберите папку для добавления**.

d. На открывшейся справа панели выберите папку, которую вы хотите исключить из области мониторинга.

e. Нажмите на кнопку **OK**.

Указанная папка добавится в список исключенных областей.

15. В окне **Область мониторинга** нажмите на кнопку **OK**.

Указанные параметры правил будут применяться к выбранной области мониторинга задачи Мониторинг файловых операций.

Анализ журналов

Этот раздел содержит информацию о задаче Анализ журналов и параметрах задачи.

О задаче Анализ журналов

В ходе выполнения задачи Анализ журналов Kaspersky Embedded Systems Security контролирует целостность защищаемой среды на основе результатов анализа журналов событий Windows. Программа информирует администратора при обнаружении признаков нетипичного поведения в системе, которые могут свидетельствовать о попытках кибератак.

Kaspersky Embedded Systems Security анализирует журналы событий Windows и выявляет нарушения в соответствии с правилами, заданными пользователем, или с параметрами эвристического анализатора, который применяется задачей для анализа журналов.

Стандартные правила и эвристический анализ

Вы можете использовать задачу Анализ журналов для контроля состояния защищаемой системы с помощью стандартных правил, осуществляющих анализ на основе встроенных эвристик. Эвристический анализатор определяет наличие аномальной активности на защищаемом устройстве, которая может являться признаком попытки атаки. Шаблоны определения аномальной активности заложены в доступных правилах в параметрах задачи.

Для задачи Анализ журналов доступно семь стандартных правил. Вы можете включать и выключать любые правила. Нельзя удалять существующие правила и создавать новые правила.

Вы можете настроить критерии срабатывания правил, которые контролируют события для следующих операций:

- обработка подбора пароля;
- обработка сетевого входа.

В параметрах задачи вы также можете настроить исключения. Эвристический анализатор не срабатывает, если вход в систему выполнен доверенным пользователем или с доверенного IP-адреса.

Kaspersky Embedded Systems Security не применяет эвристики для анализа журналов Windows, если эвристический анализатор не используется задачей. По умолчанию эвристический анализатор включен.

При срабатывании правила, программа фиксирует событие с уровнем важности *Критическое* в журнале выполнения задачи Анализ журналов.

Пользовательские правила задачи Анализ журналов

С помощью параметров правил вы можете задавать и изменять критерии срабатывания правила при обнаружении выбранных событий в указанном журнале Windows. По умолчанию список правил анализа журналов содержит четыре правила. Вы можете включать и выключать эти правила, удалять правила и редактировать их параметры.

Вы можете настроить следующие критерии срабатывания каждого правила:

- Список идентификаторов записей в журнале событий Windows.

  Правило срабатывает при создании новой записи в журнале событий Windows, если в свойствах события обнаружен идентификатор события, указанный для правила. Вы также можете добавлять и удалять идентификаторы для каждого заданного правила.

- Источник событий.

  Для каждого правила вы можете задать журнал в журнале событий Windows. Программа будет выполнять поиск записей с указанными идентификаторами событий только в этом журнале. Вы можете выбрать один из стандартных журналов (Программа, Безопасность или Система) или указать пользовательский журнал, введя его имя в поле выбора источника.

  > Программа не выполняет проверок на фактическое наличие заданного журнала в журнале событий Windows.

При срабатывании правила Kaspersky Embedded Systems Security фиксирует событие с уровнем важности Критический в журнале выполнения задачи Анализ журналов.

По умолчанию в задаче Анализ журналов применяются пользовательские правила.

> Перед запуском задачи Анализ журналов убедитесь, что политика аудита системы настроена верно. Более подробная информация приведена в статье Microsoft.

Параметры по умолчанию для задачи Анализ журналов

По умолчанию в задаче Анализ журналов используются параметры, описанные в таблице ниже. Вы можете изменять значения этих параметров.

Параметры по умолчанию для задачи Анализ журналов

Параметр	Значение по умолчанию	Описание
Применять пользовательские правила для анализа журналов	Применяется.	Пользовательские правила можно включать, отключать, добавлять или изменять.
Использовать предзаданные правила для анализа журналов	Применяется.	Можно включить или выключить эвристический анализатор, отвечающий за обнаружение аномальной активности на защищаемом устройстве.
Обработка перебора пароля	10 неудачных попыток входа в течение 300 секунд.	Можно указать количество попыток и промежуток времени, в течение которого выполнялись попытки, в качестве критерия срабатывания эвристического анализатора.
Обработка сетевого входа	00:00:00	Можно указать начало и конец временного интервала, в течение которого при выполнении попытки входа Kaspersky Embedded Systems Security расценивает данное действие как аномальную активность.
Исключения	Не применяется.	Можно указать пользователей и IP-адреса, которые не будут являться критериями срабатывания эвристического анализатора.

Расписание запуска задачи	Время первого запуска не задано.	Вы можете настроить расписание запуска задачи.

Управление правилами анализа журналов с помощью Плагина управления

В этом разделе описано добавление и настройка правил анализа журналов с помощью Плагина управления.

Настройка параметров предзаданных правил задачи

Чтобы настроить параметры стандартных правил для задачи Анализ журналов, выполните следующие действия:

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой требуется настроить параметры программы.
3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:
   - Чтобы настроить параметры программы для группы защищаемых устройств, выберите закладку **Политики** и откройте окно **Свойства: <Имя политики>**.
   - Чтобы настроить параметры программы для отдельного защищаемого устройства, выберите закладку **Устройства** и откройте окно **Параметры программы**.

     Если к устройству применяется активная политика Kaspersky Security Center, запрещающая изменение параметров программы, эти параметры недоступны для изменения в окне **Параметры программы**.
4. В разделе **Диагностика системы** в подразделе **Анализ журналов** нажмите на кнопку **Настройка**.

   Откроется окно **Анализ журналов**.
5. Выберите закладку **Предзаданные правила**.
6. Снимите или установите флажок **Использовать предзаданные правила для анализа журналов**.

   Для выполнения задачи должно быть выбрано хотя бы одно правило анализа журналов.
7. Из списка стандартных правил выберите правила, которые вы хотите применить:
   - Обнаружена возможная попытка взлома пароля с помощью подбора.
   - Обнаружены признаки компрометации журналов Windows.
   - Обнаружена подозрительная активность со стороны новой установленной службы.

- Обнаружена подозрительная аутентификация с явным указанием учетных данных.
- Обнаружены признаки атаки Kerberos forged PAC (MS14-068).
- Обнаружены подозрительные изменения привилегированной группы Администраторы.
- Обнаружена подозрительная активность во время сетевого сеанса входа.

8. Чтобы настроить параметры выбранных правил, нажмите на кнопку **Дополнительные параметры**.

   Откроется окно **Анализ журналов**.

9. В разделе **Обработка подбора пароля** укажите количество попыток и промежуток времени, в течение которого выполнялись попытки, в качестве критерия срабатывания эвристического анализатора.

10. В разделе **Обработка атипичной аутентификации** укажите начало и конец временного интервала. Выполненные в течение этого интервала попытки входа расцениваются Kaspersky Embedded Systems Security как аномальная активность.

11. Выберите закладку **Исключения**.

12. Чтобы добавить пользователей, которые будут считаться доверенными, выполните следующие действия:

    a. Нажмите на кнопку **Обзор**.

    b. Выберите пользователя.

    c. Нажмите на кнопку **ОК**.

    Указанный пользователь будет добавлен в список доверенных.

13. Чтобы добавить IP-адреса, которые будут считаться доверенными, выполните следующие действия:

    a. Введите IP-адрес.

    b. Нажмите на кнопку **Добавить**.

14. Указанный IP-адрес будет добавлен в список доверенных.

15. На закладке **Управление задачей** настройте расписание запуска задачи.

16. В окне **Анализ журналов** нажмите на кнопку **ОК**.

Параметры задачи Анализ журналов будут сохранены.

Добавление правил анализа журналов с помощью Плагина управления

Чтобы добавить и настроить новое пользовательское правило анализа журналов, выполните следующие действия:

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.

2. Выберите группу администрирования, для которой требуется настроить параметры программы.

3. В панели результатов выбранной группы администрирования выполните одно из следующих действий:

- Чтобы настроить параметры программы для группы защищаемых устройств, выберите закладку **Политики** и откройте окно **Свойства: <Имя политики>**.
- Чтобы настроить параметры программы для отдельного защищаемого устройства, выберите закладку **Устройства** и откройте окно **Параметры программы**.

  Если к устройству применяется активная политика Kaspersky Security Center, запрещающая изменение параметров программы, эти параметры недоступны для изменения в окне **Параметры программы**.

4. В разделе **Диагностика системы** в подразделе **Анализ журналов** нажмите на кнопку **Настройка**.

   Откроется окно **Анализ журналов**.

5. На закладке **Пользовательские правила** снимите или установите флажок **Применять пользовательские правила для анализа журналов**.

   Вы можете контролировать применение стандартных правил для анализа журналов. Установите флажки напротив правил, которые вы хотите применять для анализа журналов.

6. Чтобы добавить новое пользовательское правило, нажмите на кнопку **Добавить**.

   Откроется окно **Пользовательское правило**.

7. В разделе **Общие** укажите следующие данные нового правила:
   - **Имя правила**
   - **Канал**
   - **Источник**
8. В разделе **Параметры срабатывания** укажите идентификаторы событий, при обнаружении которых будет срабатывать правило.
   a. Укажите идентификатор.
   b. Нажмите на кнопку **Добавить**.

      Указанный идентификатор события будет добавлен в список. Вы можете добавлять неограниченное количество идентификаторов для каждого правила.
9. Нажмите на кнопку **ОК**.

   Правило анализа журналов добавится в список правил.

Управление правилами анализа журналов с помощью Консоли программы

В этом разделе описано добавление и настройка правил анализа журналов с помощью Консоли программы.

Настройка параметров предзаданных правил задачи

Чтобы настроить параметры работы эвристического анализатора для задачи Анализ журналов, выполните следующие действия:

1. В дереве Консоли программы разверните узел **Диагностика системы**.
2. Выберите вложенный узел **Анализ журналов**.
3. В панели результатов узла **Анализ журналов** перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи**.
4. Выберите закладку **Предзаданные правила**.
5. Снимите или установите флажок **Использовать предзаданные правила для анализа журналов**.

   Для выполнения задачи должно быть выбрано хотя бы одно правило анализа журналов.
6. Из списка стандартных правил выберите правила, которые вы хотите применить:
   - Обнаружена возможная попытка взлома пароля с помощью подбора.
   - Обнаружены признаки компрометации журналов Windows.
   - Обнаружена подозрительная активность со стороны новой установленной службы.
   - Обнаружена подозрительная аутентификация с явным указанием учетных данных.
   - Обнаружены признаки атаки Kerberos forged PAC (MS14-068).
   - Обнаружены подозрительные изменения привилегированной группы Администраторы.
   - Обнаружена подозрительная активность во время сетевого сеанса входа.
7. Чтобы настроить параметры выбранных правил, выберите закладку **Расширенные**.
8. В разделе **Обработка перебора пароля** укажите количество попыток и промежуток времени, в течение которого выполнялись попытки, в качестве критерия срабатывания эвристического анализатора.
9. В разделе **Обработка сетевого входа** укажите начало и конец временного интервала. Выполненные в течение этого интервала попытки входа расцениваются Kaspersky Embedded Systems Security как аномальная активность.
10. Выберите закладку **Исключения**.
11. Чтобы добавить пользователей, которые будут считаться доверенными, выполните следующие действия:
    a. Нажмите на кнопку **Обзор**.
    b. Выберите пользователя.
    c. Нажмите на кнопку **OK**.

Указанный пользователь будет добавлен в список доверенных.

12. Чтобы добавить IP-адреса, которые будут считаться доверенными, выполните следующие действия:

    a. Введите IP-адрес.

    b. Нажмите на кнопку **Добавить**.

    Указанный IP-адрес будет добавлен в список доверенных.

13. Выберите закладки **Расписание** и **Дополнительно**, чтобы настроить расписание запуска задачи.

14. В окне **Параметры задачи** нажмите на кнопку **ОК**.

    Параметры задачи Анализ журналов будут сохранены.

Добавление правил анализа журналов с помощью Консоли программы

Чтобы добавить и настроить пользовательское правило анализа журналов, выполните следующие действия:

1. В дереве Консоли программы разверните узел **Диагностика системы**.

2. Выберите вложенный узел **Анализ журналов**.

3. В панели результатов узла **Анализ журналов** перейдите по ссылке **Правила анализа журналов**.

   Откроется окно **Правила анализа журналов**.

4. Снимите или установите флажок **Применять пользовательские правила для анализа журналов. Настроенные параметры правил не применяются, если флажок снят**.

   Вы можете контролировать применение стандартных правил в задаче Анализ журналов. Установите флажки напротив правил, которые вы хотите применять для анализа журналов.

5. Чтобы создать пользовательское правило, выполните следующие действия:

   a. Введите имя нового правила.

   b. Нажмите на кнопку **Добавить**.

   Созданное правило добавится в общий список правил.

6. Чтобы настроить любое правило, выполните следующие действия:

   a. Выберите правило в списке.

   В правой области окна на закладке **Комментарий** отобразится общая информация о правиле.

   Комментарии для нового правила пусты.

   b. Выберите закладку **Параметры правила**.

7. В разделе **Общие** укажите следующие данные нового правила:

- **Имя правила**
- **Канал**
- **Источник**

8. В разделе **Источник события** укажите идентификаторы событий, при обнаружении которых будет срабатывать правило.

   a. Укажите идентификатор события.

   b. Нажмите на кнопку **Добавить**.

      Указанный идентификатор события будет добавлен в список. Вы можете добавлять неограниченное количество идентификаторов для каждого правила.

9. Нажмите на кнопку **Сохранить**.

   Настроенные параметры правил анализа журналов будут применены.

Управление правилами анализа журналов с помощью Веб-плагина

Чтобы добавить и настроить правила анализа журналов с помощью Веб-плагина, выполните следующие действия:

1. В главном окне веб-консоли выберите **Устройства** → **Политики и профили**.
2. Выберите политику, которую вы хотите настроить.
3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.
4. Выберите раздел **Диагностика системы**.
5. Нажмите на кнопку **Параметры** в подразделе **Анализ журналов**.
6. Настройте параметры, приведены в следующей таблице.

Параметры задачи Анализ журналов

Параметр	Описание
Применять пользовательские правила для анализа журналов	Пользовательские правила можно включать, отключать, добавлять или изменять. Этот параметр доступен в таблице со списком пользовательских правил.
Использовать предзаданные правила для анализа журналов	Можно включить или выключить эвристический анализатор, отвечающий за обнаружение аномальной активности на защищаемом устройстве. Этот параметр доступен в таблице со списком пользовательских правил.
Количество попыток	Можно указать количество попыток и промежуток времени, в течение которого выполнялись попытки, в качестве критерия срабатывания эвристического анализатора.
Конец интервала	Можно указать начало и конец временного интервала, в течение которого при выполнении попытки входа Kaspersky Embedded Systems Security расценивает данное действие как аномальную активность.

Исключения	Можно указать пользователей, которые не будут являться критериями срабатывания эвристического анализатора.
Исключения IP-адресов	Можно указать IP-адреса, которые не будут являться критериями срабатывания эвристического анализатора.
Управление задачами	Вы можете настроить расписание запуска задачи.

Проверка по требованию

Этот раздел содержит информацию о задачах проверки по требованию, а также инструкции по настройке параметров задач проверки по требованию и по настройке параметров безопасности защищаемого устройства.

О задачах проверки по требованию

Kaspersky Embedded Systems Security проверяет указанную область на наличие вирусов и других угроз компьютерной безопасности. Kaspersky Embedded Systems Security проверяет файлы и оперативную память защищаемого устройства, а также объекты автозапуска.

В Kaspersky Embedded Systems Security предусмотрены следующие задачи проверки по требованию:

- Задача Проверка при старте операционной системы выполняется каждый раз при запуске Kaspersky Embedded Systems Security. Kaspersky Embedded Systems Security проверяет загрузочные секторы и основные загрузочные записи жестких и съемных дисков, системную память и память процессов. Каждый раз при запуске задачи Kaspersky Embedded Systems Security создает копию незараженных загрузочных секторов. Если при следующем запуске задачи в этих секторах обнаруживается угроза, программа заменяет их резервными копиями.

- По умолчанию задача Проверка важных областей выполняется еженедельно по расписанию. Kaspersky Embedded Systems Security проверяет объекты, расположенные в важных областях операционной системы: объекты автозапуска, загрузочные секторы и основные загрузочные записи жестких и съемных дисков, системную память и память процессов. Программа проверяет файлы в системных папках, например, в папке %windir%\system32. Kaspersky Embedded Systems Security применяет параметры безопасности, соответствующие рекомендуемому уровню. Вы можете изменять параметры задачи Проверка важных областей.

- Задача Проверка объектов на карантине по умолчанию выполняется по расписанию после каждого обновления баз программы. Область действия задачи Проверка объектов на карантине изменять нельзя.

- Задача Проверка целостности программы выполняется ежедневно. Она обеспечивает проверку модулей Kaspersky Embedded Systems Security на предмет наличия повреждений или изменений. Проверяется папка установки программы. Статистика выполнения задачи содержит сведения о количестве проверенных и поврежденных модулей. Значения параметров задачи устанавливаются по умолчанию и не доступны для изменения. Вы можете настраивать расписание запуска задачи.

Кроме того, вы можете создать пользовательскую задачу проверки по требованию, например, задачу проверки папок общего доступа на защищаемом устройстве.

Kaspersky Embedded Systems Security может одновременно выполнять несколько задач проверки по требованию.

Об области проверки и параметрах безопасности задачи

В Консоли программы область проверки выбранной задачи проверки по требованию представляет собой дерево или список файловых ресурсов защищаемого устройства, которые может контролировать Kaspersky Embedded Systems Security. По умолчанию сетевые файловые ресурсы защищаемого устройства отображаются в виде списка.

В Плагине управления доступно только представление в виде списка.

Чтобы включить отображение сетевых файловых ресурсов в виде дерева в Консоли программы,

в раскрывающемся списке, расположенном в левом верхнем углу окна **Настройка области проверки**, выберите элемент **Показывать в виде дерева**.

Элементы и узлы в дереве или списке файловых ресурсов защищаемого устройства отображаются следующим образом:

☑ – узел включен в область проверки.

☐ – узел исключен из области проверки.

▣ – по крайней мере один из узлов, вложенных в этот узел, исключен из области проверки, или параметры безопасности вложенных узлов отличаются от параметров безопасности этого узла (только для режима отображения в виде дерева).

Значок ▣ отображается, если выбраны все вложенные узлы, но не выбран родительский узел. В этом случае изменения состава файлов и папок родительского узла не учитываются автоматически при формировании области проверки для выбранного вложенного узла.

С помощью Консоли программы можно также добавлять виртуальные диски в область проверки. Имена виртуальных узлов отображаются шрифтом синего цвета.

Параметры безопасности

В выбранной задаче проверки по требованию можно изменять заданные по умолчанию параметры безопасности, настроив их либо едиными для всей области защиты или проверки, либо различными для разных узлов или элементов в дереве или списке файловых ресурсов устройства.

Параметры безопасности, настроенные для выбранного родительского узла, автоматически применяются ко всем вложенным узлам. Параметры безопасности родительского узла не применяются к вложенному узлу, который настраивается отдельно.

Вы можете настроить параметры выбранной области защиты или проверки одним из следующих способов:

- выбрать один из трех стандартных уровней безопасности (**Максимальное быстродействие**, **Рекомендуемый** или **Максимальная защита**);
- вручную изменить параметры безопасности для выбранных узлов или элементов в дереве или списке файловых ресурсов защищаемого устройства (уровень безопасности примет значение **Другой**).

Вы можете сохранить набор параметров узла в шаблон, чтобы потом применять этот шаблон для других узлов.

Стандартные области проверки

Дерево или список файловых ресурсов зачищаемого устройства для выбранной задачи проверки по требованию отображается в окне **Настройка области проверки**.

В дереве или списке файловых ресурсов отображаются узлы, к которым у вас есть доступ на чтение в соответствии с настроенными параметрами безопасности Microsoft Windows.

В Kaspersky Embedded Systems Security предусмотрены следующие стандартные области проверки:

- **Мой компьютер**. Kaspersky Embedded Systems Security проверяет защищаемое устройство целиком.
- **Локальные жесткие диски**. Kaspersky Embedded Systems Security проверяет объекты на жестких дисках защищаемого устройства. Вы можете включать в область проверки или исключать из нее все жесткие диски, а также отдельные диски, папки или файлы.
- **Съемные диски**. Kaspersky Embedded Systems Security проверяет файлы на внешних устройствах, таких как компакт-диски или съемные диски. Вы можете включать в область проверки или исключать из нее все съемные диски, а также отдельные диски, папки или файлы.
- **Сетевое окружение**. Вы можете добавлять в область проверки сетевые папки или файлы, указывая пути к ним в формате UNC (Universal Naming Convention). Учетная запись, используемая для запуска задачи, должна обладать правами доступа к добавленным сетевым папкам или файлам. По умолчанию задачи проверки по требованию выполняются с правами системной учетной записи.

  Подключенные сетевые диски также не отображаются в дереве файловых ресурсов защищаемого устройства. Чтобы включить в область проверки объекты на сетевом диске, укажите путь к папке, соответствующей этому сетевому диску, в формате UNC (Universal Naming Convention).

- **Системная память**. Kaspersky Embedded Systems Security проверяет исполняемые файлы и модули процессов, которые выполняются в операционной системе на момент проверки.
- **Объекты автозапуска**. Kaspersky Embedded Systems Security проверяет объекты, на которые ссылаются ключи реестра и конфигурационные файлы, например, WIN.INI или SYSTEM.INI, а также программные модули, которые автоматически запускаются при запуске защищаемого устройства.
- **Папки общего доступа**. Вы можете включать в область проверки папки общего доступа на защищаемом устройстве.
- **Виртуальные диски**. Вы можете включать в область проверки виртуальные папки, файлы и диски, подключенные к защищаемому устройству, например, общие диски кластера.

  Виртуальные диски, созданные с помощью команды SUBST, не отображаются в дереве файловых ресурсов защищаемого устройства в Консоли программы. Чтобы проверить объекты на виртуальном диске, включите в область проверки папку на защищаемом устройстве, с которой связан этот виртуальный диск.

Стандартные области проверки по умолчанию отображаются в дереве сетевых файловых ресурсов. Они доступны для добавления в список сетевых файловых ресурсов при его формировании в параметрах области проверки.

По умолчанию задачи проверки по требованию выполняются в следующих областях:

- Задача Проверка при старте операционной системы:
  - **Локальные жесткие диски**
  - **Съемные диски**

- **Системная память**

- Задача Проверка важных областей:
  - **Локальные жесткие диски** (исключая папки Windows)
  - **Съемные диски**
  - **Системная память**
  - **Объекты автозапуска**
- Прочие задачи:
  - **Локальные жесткие диски** (исключая папки Windows)
  - **Съемные диски**
  - **Системная память**
  - **Объекты автозапуска**
  - **Папки общего доступа**

Проверка файлов в интернет-хранилище

Об облачных файлах

Kaspersky Embedded Systems Security может взаимодействовать с облачными файлами Microsoft OneDrive. Программа поддерживает новую функцию "файлы из OneDrive по запросу" (OneDrive Files On-Demand).

> Kaspersky Embedded Systems Security не поддерживает другие интернет-хранилища.

Функция "файлы из OneDrive по запросу" помогает получить доступ к вашим файлам OneDrive без необходимости загружать их и занимать дисковое пространство на вашем устройстве. При необходимости можно загрузить файлы на жесткий диск вашего устройства.

Когда функция "файлы из OneDrive по запросу" включена, рядом с каждым файлом в графе **Статус** в проводнике Windows отображается значок статуса. Файл может иметь один из следующих статусов:

– этот значок показывает, что файл *доступен только через интернет*. Файлы, доступные только через интернет, не хранятся физически на жестком диске. Если ваше устройство не подключено к интернету, вы не сможете открывать файлы, доступные только через интернет.

– этот значок показывает, что файл *доступен локально*. Он отображается, если вы открыли файл, доступный только через интернет, и он загрузился на ваше устройство. Доступные локально файлы можно открывать в любое время, даже без доступа в интернет. Чтобы освободить пространство, вы можете снова сделать файл доступным только через интернет ( ).

– этот значок показывает, что файл *хранится на жестком диске и всегда доступен*.

Проверка облачных файлов

Kaspersky Embedded Systems Security может выполнять проверку только облачных файлов, сохраненных локально на защищаемом устройстве. Такие файлы OneDrive имеют статус или . Проверка файлов со статусом не выполняется, поскольку физически они не хранятся на защищаемом устройстве.

Во время проверки Kaspersky Embedded Systems Security не выполняет автоматическую загрузку файлов со статусом из облачного хранилища, даже если они включены в область проверки.

Обработка облачных файлов выполняется различными задачами Kaspersky Embedded Systems Security в различных сценариях, в зависимости от типа задачи:

- Постоянная проверка облачных файлов: вы можете добавить папки, содержащие облачные файлы, в область задачи Постоянная защита файлов. Проверка файла выполняется, когда пользователь открывает его. Если пользователь открывает файл со статусом , этот файл загружается и становится доступным локально; его статус меняется на . Поэтому этот файл может быть обработан задачей Постоянная защита файлов.

- Проверка облачных файлов по требованию: вы можете добавить папки, содержащие облачные файлы, в область проверки задачи проверки по требованию. Задача выполняет проверку файлов со статусами и . Если в области проверки задачи обнаружены файлы со статусом , эти файлы будут пропущены при проверке, а в журнале выполнения задачи будет зарегистрировано информационное событие, показывающее, что проверяемый файл является временной заменой облачного файла и отсутствует на локальном диске.

- Формирование и использование правил контроля запуска программ: можно создавать разрешающие и запрещающие правила для файлов со статусами и с помощью задачи Формирование правил контроля запуска программ. Задача Контроль запуска программ обрабатывает и блокирует облачные файлы в соответствии с принципом запрета по умолчанию и созданными правилами.

  Задача Контроль запуска программ блокирует запуск всех облачных файлов, независимо от статуса файла. Файлы со статусом не входят в область формирования правила, поскольку они не хранятся физически на жестком диске. Для таких файлов невозможно создать разрешающих правил, поэтому они подчиняются принципу запрета по умолчанию.

Если в облачном файле OneDrive обнаружена угроза, программа применяет действие, указанное в параметрах задачи, выполняющей проверку. Таким образом, файл может быть удален, вылечен, помещен на карантин или в резервное хранилище.

При изменении локальные файлы синхронизируются с копиями в облачном хранилище OneDrive в соответствии с принципами, описанными в документации к Microsoft OneDrive.

Стандартные уровни безопасности

Параметры безопасности **Использовать технологию iChecker**, **Использовать технологию iSwift**, **Использовать эвристический анализатор** и **Проверять подпись Microsoft у файлов** не входят в набор параметров стандартных уровней безопасности. При изменении параметров **Использовать технологию iChecker**, **Использовать технологию iSwift**, **Использовать эвристический анализатор** и **Проверять подпись Microsoft у файлов**, выбранный вами стандартный уровень безопасности не изменится.

Для выбранного узла в дереве файловых ресурсов узла можно задать один из трех стандартных уровней безопасности: **Максимальное быстродействие**, **Рекомендуемый** или **Максимальная защита**. Каждый из этих уровней имеет свои стандартные параметры безопасности (см. таблицу ниже).

Максимальное быстродействие

Уровень безопасности **Максимальное быстродействие** рекомендуется применять, если в вашей сети, наряду с использованием Kaspersky Embedded Systems Security на защищаемых устройствах, применяются дополнительные меры безопасности, например, сетевые экраны и политики безопасности.

Рекомендуемый

Уровень безопасности **Рекомендуемый** обеспечивает оптимальное сочетание качества защиты и влияния на производительность устройств. Этот уровень рекомендован специалистами "Лаборатории Касперского" как достаточный для защиты устройств в большинстве сетей организаций. Уровень безопасности **Рекомендуемый** установлен по умолчанию.

Максимальная защита

Уровень безопасности **Максимальная защита** рекомендуется применять, если предъявляются повышенные требования к безопасности устройств в сети организации.

Стандартные уровни безопасности и соответствующие им значения параметров безопасности

Параметры	Уровень безопасности		
	Максимальное быстродействие	**Рекомендуемый**	**Максимальная защита**
Проверка объектов	По формату	Все объекты	Все объекты
Проверка только новых и измененных файлов	Включена	Выключено	Выключено
Действия над зараженными и другими обнаруженными объектами	Лечить. Удалить, если не удалось вылечить.	Выполнять рекомендованное действие (Лечить. Удалить, если не удалось вылечить.)	Лечить. Удалить, если не удалось вылечить.
Действия над возможно зараженными объектами	Карантин	Выполнять рекомендованное действие (Поместить на карантин)	Карантин
Исключать файлы	Нет	Нет	Нет
Не обнаруживать	Нет	Нет	Нет
Останавливать проверку, если она длится более (сек.)	60 сек.	Нет	Нет

Не проверять составные объекты размером более (МБ)	8 МБ	Нет	Нет
Альтернативные потоки NTFS	Да	Да	Да
Загрузочные секторы дисков и MBR	Да	Да	Да
Проверка составных объектов	• SFX-архивы* • Упакованные объекты* • Вложенные OLE-объекты* * Только новые и измененные	• Архивы* • SFX-архивы* • Упакованные объекты* • Вложенные OLE-объекты* * Все объекты	• Архивы* • SFX-архивы* • Почтовые базы* • Файлы почтовых форматов* • Упакованные объекты* • Вложенные OLE-объекты* * Все объекты

Проверка съемных дисков

Вы можете настроить проверку съемных дисков, подключенных к защищаемому устройству по USB.

Kaspersky Embedded Systems Security выполняет проверку съемного диска с помощью задачи проверки по требованию. Программа автоматически создает новую задачу Проверка по требованию в момент подключения съемного диска и удаляет созданную задачу по завершении проверки. Созданная задача выполняется со стандартным уровнем безопасности, указанным для проверки съемных дисков. Вы не можете настроить параметры временной задачи проверки по требованию.

Если программа Kaspersky Embedded Systems Security была установлена без антивирусных баз, проверка съемных дисков будет недоступна.

Kaspersky Embedded Systems Security запускает проверку съемных дисков при их регистрации в операционной системе в качестве внешних устройств, подключаемых по USB. Программа не выполняет проверку съемного диска, если его подключение было заблокировано задачей Контроль устройств. Программа не выполняет проверку MTP-подключаемых мобильных устройств.

Kaspersky Embedded Systems Security не блокирует доступ к съемному диску на время проверки.

Результаты проверки каждого съемного диска доступны в журнале выполнения задачи проверки по требованию, созданной при подключении этого съемного диска.

Вы можете изменять значения параметров компонента Проверка съемных дисков (см. таблицу ниже).

Параметры проверки съемных дисков

Параметр	Значение по умолчанию	Описание
Проверять съемные диски при их подключении по USB	Флажок снят	Вы можете включать или выключать проверку съемных дисков при их подключении к защищаемому устройству по USB.
Проверять, если объем содержащихся на диске данных не превышает порог (МБ)	1024 МБ	Вы можете уменьшить область срабатывания компонента, указав максимальный объем данных на проверяемом диске. Kaspersky Embedded Systems Security не выполняет проверку съемного диска, если объем содержащихся на нем данных превышает указанное значение.
Запускать проверку с уровнем безопасности	Максимальная защита	Вы можете настраивать параметры создаваемых задач проверки по требованию, выбирая один из трех уровней безопасности: • **Максимальная защита** • **Рекомендуемый** • **Максимальное быстродействие** Алгоритм действий при обнаружении зараженных, возможно зараженных и других объектов, а также другие параметры проверки для каждого уровня безопасности соответствуют стандартным уровням безопасности в задачах проверки по требованию.

О задаче Мониторинг целостности файлов на основе эталона

Во время выполнения задачи Мониторинг целостности файлов на основе эталона Kaspersky Embedded Systems Security не проверяет заблокированные файлы, папки, ярлыки файлов и облачные файлы.

В задаче Мониторинг целостности файлов на основе эталона выполняется контроль целостности файлов в области мониторинга посредством сравнения хеша файлов (MD5 или SHA256) с эталонным значением.

При первом запуске задачи Мониторинг целостности файлов на основе эталона, Kaspersky Embedded Systems Security создает эталон, рассчитывая и сохраняя хеш для файлов в области мониторинга задачи. При изменении области задачи Мониторинг целостности файлов на основе эталона, Kaspersky Embedded Systems Security обновляет эталон при следующем запуске задачи Мониторинг целостности файлов на основе эталона, рассчитывая и сохраняя хеш для файлов в области мониторинга задачи. При удалении задачи Мониторинг целостности файлов на основе эталона, Kaspersky Embedded Systems Security удаляет эталон этой задачи.

С помощью командной строки можно удалить эталон, не удаляя задачу Мониторинг целостности файлов на основе эталона.

Задача Мониторинг целостности файлов на основе эталона отслеживает следующие изменения файлов в области мониторинга:

- область мониторинга содержит файл, который отсутствует в эталоне;
- в области мониторинга отсутствует файл, который присутствует в эталоне;
- хеш файла в области мониторинга отличается от хеша этого файла в эталоне.

Задача Мониторинг целостности файлов на основе эталона не отслеживает изменения атрибутов файлов и изменения альтернативных потоков.

Если файл или папка недоступны, Kaspersky Embedded Systems Security не добавляет этот файл или папку в эталон при создании, а формирует событие о невозможности рассчитать хеш при запуске задачи Мониторинг целостности файлов на основе эталона.

Файл или папка могут быть недоступны по следующим причинам:

- указанный путь не существует;
- тип файлов, указанный в маске, отсутствует по указанному пути;
- указанный файл заблокирован;
- указан пустой файл.

Включение запуска задачи проверки по требованию из контекстного меню

Можно включить запуск задачи проверки по требованию из контекстного меню файла в проводнике Windows.

Чтобы включить запуск задачи проверки по требованию из контекстного меню, выполните следующие действия:

1. Создайте следующие REG-файлы:

```
Windows Registry Editor Version 5.0.0
[HKEY_CLASSES_ROOT\Directory\shell\kess\command]
@="C:\\Temp\\scan.cmd \"%1\""
[HKEY_CLASSES_ROOT\*\shell\kess\command]
@="C:\\Temp\\scan.cmd \"%1\""
[HKEY_CLASSES_ROOT\Directory\shell\kess]
@="Проверить с помощью Kaspersky Embedded Systems Security\"
"Icon"="\"C:\\Program Files (x86)\\Kaspersky Lab\\Kaspersky Embedded Systems Security\\kavtrayr.dll\",0"
[HKEY_CLASSES_ROOT\Directory\shell\kess\DefaultIcon]
@="\"C:\\Program Files (x86)\\Kaspersky Lab\\Kaspersky Embedded Systems Security\\kavtrayr.dll\",0"
[HKEY_CLASSES_ROOT\*\shell\kess]
@="Проверить с помощью Kaspersky Embedded Systems Security\"
```

```
"Icon"="\"C:\\Program Files (x86)\\Kaspersky Lab\\Kaspersky Embedded Systems
Security\\kavtrayr.dll\",0"

[HKEY_CLASSES_ROOT\*\shell\kess\DefaultIcon]
@="\"C:\\Program Files (x86)\\Kaspersky Lab\\Kaspersky Embedded Systems
Security\\kavtrayr.dll\",0"

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\AppCompatFlags\Layers]

"C:\\Program Files (x86)\\Kaspersky Lab\\Kaspersky Embedded Systems
Security\\kavshell.exe"="~ RUNASADMIN"
```

Необходимо указать реальное местоположение папки, в которую установлена программа Kaspersky Embedded Systems Security.

2. Создайте файл `scan.cmd` со следующим содержимым:

```
@echo off
set LOGNAME=%RANDOM%

"C:\Program Files (x86)\Kaspersky Lab\Kaspersky Embedded Systems
Security\kavshell.exe" scan "%~1" /W:c:\temp\%LOGNAME%.txt

echo Выполняется проверка...
type c:\temp\%LOGNAME%.txt
del c:\temp\%LOGNAME%.txt

timeout /t -1
```

Файл `scan.cmd` должен содержать следующую информацию:

- Местоположение файла `kavshell.exe`.
- Местоположение временного файла, содержащего результаты проверки.
- Параметры команды `KAVSHELL SCAN`.
- Значение времени ожидания закрытия окна консоли после завершения задачи.

3. Скопируйте файл `scan.cmd` в папку, указанную в REG-файле как значение параметра `[HKEY_CLASSES_ROOT\Directory\shell\kess\command]`.

В примере указана папка `C:\Temp`.

Перезагрузка операционной системы не требуется.

Заданные по умолчанию параметры задач проверки по требованию

По умолчанию задачи проверки по требованию имеют параметры, описанные в таблице ниже. Вы можете настраивать системные и пользовательские задачи проверки по требованию.

Заданные по умолчанию параметры задач проверки по требованию

Параметр	Значение по умолчанию	Описание
Область	Применяется в следующих	Вы можете изменить область проверки. Область

проверки	системных и пользовательских задачах: • **Проверка при старте операционной системы**: защищаемое устройство целиком, за исключением папок общего доступа и объектов автозапуска. • **Проверка важных областей**: защищаемое устройство целиком, за исключением папок общего доступа и некоторых файлов операционной системы. • **Проверка по требованию** (пользовательские задачи): защищаемое устройство целиком.	проверки нельзя настроить для системных задач **Проверка объектов на карантине** и **Проверка целостности программы**.
Параметры безопасности	Единые для всей области проверки, соответствуют уровню безопасности **Рекомендуемый**.	Для узлов, выбранных в дереве или списке файловых ресурсов защищаемого устройства, можно выполнить следующие действия: • выбрать другой стандартный уровень безопасности; • вручную изменить параметры безопасности. Вы можете сохранить набор параметров безопасности выбранного узла как шаблон, чтобы потом применить его для другого узла.
Использовать эвристический анализатор	Применяется с уровнем анализа **Средний** для задач Проверка важных областей и Проверка при старте операционной системы, а также для пользовательских задач. Применяется с уровнем анализа **Глубокий** для задачи Проверка объектов на карантине.	Вы можете включать и выключать применение эвристического анализатора и регулировать уровень анализа. Вы не можете настроить уровень анализа для задачи Проверка объектов на карантине. Эвристический анализатор не используется в задачах Проверка целостности программы и Мониторинг целостности файлов на основе эталона.
Применять доверенную зону	Применяется (не применяется для задачи Проверка объектов на карантине)	Единый список исключений, который можно применять в выбранных задачах.
Использовать KSN для проверки	Применяется.	Вы можете увеличить эффективность защиты устройства с помощью инфраструктуры облачных служб Kaspersky Security Network.
Параметры запуска задачи с определенными правами	Задача запускается с правами системной учетной записи.	Вы можете изменять параметры запуска задач с правами учетных записей для всех системных и пользовательских задач проверки по требованию, кроме задач Проверка объектов на карантине и Проверка целостности программы.
Выполнять задачу в фоновом	Не применяется	Вы можете настраивать приоритетность выполнения задач проверки по требованию.

режиме (низкий приоритет)		
Расписание запуска задачи	Применяется в системных задачах: • Проверка при старте операционной системы – **При запуске программы**; • Проверка важных областей – **Еженедельно**; • Проверка объектов на карантине – **После обновления баз программы**; • Проверка целостности программы – **Ежесуточно**. Не применяется во вновь созданных пользовательских задачах.	Можно настроить параметры для запуска задачи по расписанию.
Регистрация выполнения проверки и обновление статуса защиты устройства	Статус защиты устройства обновляется еженедельно после выполнения задачи Проверка важных областей.	Вы можете настраивать параметры регистрации выполнения проверки важных областей следующими способами: • изменяя параметры расписания запуска задачи Проверка важных областей; • изменяя область проверки задачи Проверка важных областей; • создавая пользовательские задачи проверки по требованию.

Управление задачами проверки по требованию с помощью Плагина управления

В этом разделе описана навигация в интерфейсе Плагина управления и настройка параметров задачи для защищаемых устройств в сети.

Навигация

В этом разделе описан переход к требуемым параметрам задачи с помощью интерфейса.

Переход к мастеру создания задачи проверки по требованию

Чтобы создать пользовательскую задачу проверки по требованию, выполните следующие действия:

1. Для создания локальной задачи:

   a. Разверните узел **Управляемые устройства** в Консоли администрирования Kaspersky Security Center.

   b. Выберите группу администрирования, к которой принадлежит защищаемое устройство.

   c. В панели результатов на закладке **Устройства** откройте контекстное меню защищаемого устройства.

   d. Выберите пункт меню **Свойства**.

   e. В открывшемся окне в разделе **Задачи** нажмите на кнопку **Добавить**.

   Откроется окно **Мастер создания задачи**.

2. Для создания групповой задачи:

   a. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.

   b. Выберите группу администрирования, для которой требуется создать задачу.

   c. Выберите закладку **Задачи**.

   d. Нажмите на кнопку **Создать задачу**.

   Откроется окно **Мастер создания задачи**.

3. Чтобы создать задачу для произвольного набора защищаемых устройств, выполните следующие действия:

   a. В Консоли администрирования Kaspersky Security Center в панели результатов узла **Выборки устройств** нажмите на кнопку **Запустить выборку**, чтобы выбрать устройства.

   b. Выберите закладку **Результаты выборки "имя выборки"**.

   c. В раскрывающемся списке **Сделать выборку** выберите вариант **Создать задачу для результатов выборки**.

   Откроется окно **Мастер создания задачи**.

4. Выберите задачу **Проверка по требованию** в списке доступных задач для Kaspersky Embedded Systems Security.

5. Нажмите на кнопку **Далее**.

   Откроется окно **Настройка**.

Настройте параметры задачи в соответствии с вашими требованиями.

Чтобы настроить задачу проверки по требованию,

откройте окно свойств задачи двойным щелчком мыши на названии задачи в списке задач Kaspersky Security Center.

Откроется окно **Свойства: Проверка по требованию**.

Переход к свойствам задачи проверки по требованию

Чтобы перейти к свойствам программы для задачи проверки по требованию для отдельного защищаемого устройства, выполните следующие действия:

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, к которой принадлежит защищаемое устройство.
3. Выберите закладку **Устройства**.
4. Дважды щелкните мышью по имени защищаемого устройства, для которого вы хотите настроить область проверки.

   Откроется окно **Свойства: <Имя защищаемого устройства>**.
5. Выберите раздел **Задачи**.
6. В списке задач, созданных для устройства, выберите созданную задачу проверки по требованию.
7. Нажмите на кнопку **Свойства**.

   Откроется окно **Свойства: Проверка по требованию**.

Настройте параметры задачи в соответствии с вашими требованиями.

Создание задачи проверки по требованию

Чтобы создать пользовательскую задачу проверки по требованию, выполните следующие действия:

1. Откройте окно **Настройка** в мастере создания задачи.
2. Выберите требуемый **Способ создания задачи**.
3. Нажмите на кнопку **Далее**.
4. В окне **Область проверки** сформируйте область проверки.

   По умолчанию область проверки включает критические области защищаемого устройства. Проверяемые области отображаются в таблице помеченными значком ☑. Области, являющиеся исключениями из проверки, отображаются в таблице помеченными значком ☐.

   Вы можете изменять область проверки: включать в нее отдельные стандартные области, диски, папки, сетевые объекты и файлы и устанавливать особые параметры безопасности для каждой из добавленных областей.

   - Чтобы исключить из проверки все важные области, откройте контекстное меню на каждой из строк и выберите **Удалить область**.

- Чтобы включить стандартную область проверки, диск, папку, сетевой объект или файл в область проверки, выполните следующие действия:

  a. Откройте контекстное меню таблицы **Область проверки** и выберите **Добавить область** или нажмите на кнопку **Добавить**.

  b. В окне **Добавление в область проверки** выберите стандартную область в списке **Предопределенная область**, укажите диск, папку, сетевой объект или файл на защищаемом устройстве или другом защищаемом устройстве в сети и нажмите на кнопку **ОК**.

- Чтобы исключить вложенные папки или файлы из области проверки, выберите добавленную папку (диск) в окне мастера **Область проверки**:

  a. Откройте контекстное меню и выберите пункт **Настроить**.

  b. Нажмите на кнопку **Настройка** в окне **Уровень безопасности**.

  c. На закладке **Общие** в окне **Настройка проверки по требованию** снимите флажки **Вложенные папки** и **Вложенные файлы**.

- Чтобы изменить параметры безопасности области проверки, выполните следующие действия:

  a. Откройте контекстное меню области проверки, параметры которой требуется изменить, и выберите пункт **Настроить**.

  b. В окне **Настройка проверки по требованию** выберите один из стандартных уровней безопасности или нажмите на кнопку **Настройка**, чтобы настроить параметры безопасности вручную.

  Параметры безопасности настраиваются таким же образом, как и для задачи Постоянная защита файлов.

- Чтобы пропускать вложенные объекты в добавленной области проверки, выполните следующие действия:

  a. Откройте контекстное меню таблицы **Область проверки** и выберите пункт **Добавить исключение**.

  b. Укажите объекты, которые вы хотите исключить: выберите стандартную область в списке **Предопределенная область**, укажите диск, папку, сетевой объект или файл на защищаемом устройстве или другом защищаемом устройстве сети.

  c. Нажмите на кнопку **ОК**.

5. В окне **Параметры** настройте эвристический анализатор и интеграцию с другими компонентами:

- Настройте применение эвристического анализатора.

- Установите флажок **Применять доверенную зону**, если вы хотите исключить из области проверки задачи объекты, входящие в доверенную зону.

- Установите флажок **Использовать KSN для проверки**, если вы хотите использовать облачные службы Kaspersky Security Network для задачи.

- Чтобы присвоить рабочему процессу, в котором будет выполняться задача, приоритет *Низкий*, в окне **Параметры** установите флажок **Выполнять задачу в фоновом режиме**.

По умолчанию рабочие процессы, в которых выполняются задачи Kaspersky Embedded Systems Security, имеют приоритет *Средний*.

- Чтобы использовать создаваемую задачу в качестве задачи Проверка важных областей, в окне **Параметры** установите флажок **Считать выполнение задачи проверкой важных областей**.

6. Нажмите на кнопку **Далее**.
7. В окне **Расписание** укажите параметры запуска задачи по расписанию.
8. Нажмите на кнопку **Далее**.
9. В окне **Выбор учетной записи для запуска задачи** укажите требуемую учетную запись.
10. Нажмите на кнопку **Далее**.
11. Укажите название задачи.
12. Нажмите на кнопку **Далее**.

    Название задачи не должно быть длиннее 100 символов и не должно содержать следующие символы: " * < > & \ : |

    Откроется окно **Завершение создания задачи**.
13. По завершении работы мастера можно запустить задачу, установив флажок **Запустить задачу после завершения работы мастера**.
14. Нажмите на кнопку **Завершить**, чтобы завершить создание задачи.

Будет создана новая задача проверки по требованию для выбранного защищаемого устройства или группы защищаемых устройств.

Присвоение задаче проверки по требованию статуса Проверка важных областей

По умолчанию Kaspersky Security Center присваивает защищаемому устройству статус *Предупреждение*, если задача Проверка важных областей выполняется реже, чем указано параметром для порога формирования события в Kaspersky Embedded Systems Security – *Проверка важных областей защищаемого устройства давно не выполнялась*.

Чтобы настроить проверку всех защищаемых устройств, входящих в одну группу администрирования, выполните следующие действия:

1. Создайте групповую задачу проверки по требованию.
2. В окне **Параметры** мастера создания задачи установите флажок **Считать выполнение задачи проверкой важных областей**. Указанные параметры задачи (область проверки и параметры безопасности) будут применены ко всем защищаемым устройствам в группе. Настройте расписание задачи.

Флажок **Считать выполнение задачи проверкой важных областей** можно установить при создании задачи проверки по требованию для группы защищаемых устройств или позднее в окне **Свойства: <Название задачи>**.

3. С помощью новой или существующей политики выключите запуск по расписанию системных задач проверки по требованию для группы защищаемых устройств.

С этого момента Сервер администрирования Kaspersky Security Center будет оценивать состояние безопасности защищаемого устройства и уведомлять о нем по результатам последнего выполнения задачи со статусом Проверка важных областей, а не по результатам выполнения системной задачи Проверка важных областей.

Вы можете присваивать статус *Проверка важных областей* как групповым задачам проверки по требованию, так и задачам для групп защищаемых устройств.

В Консоли программы можно также просмотреть, имеет ли задача проверки по требованию статус Проверка важных областей.

В Консоли программы флажок **Считать выполнение задачи проверкой важных областей** отображается в свойствах задачи, но не доступен для редактирования.

Выполнение задач проверки по требованию в фоновом режиме

По умолчанию процессы, в которых выполняются задачи Kaspersky Embedded Systems Security, имеют приоритет *Средний*.

Вы можете присвоить процессу, в котором будет выполняться задача проверки по требованию, приоритет *Низкий*. Понижение приоритета процесса увеличивает время выполнения задачи, но может положительно повлиять на скорость выполнения процессов других запущенных программ.

В одном рабочем процессе с низким приоритетом может выполняться несколько задач в фоновом режиме. Можно указать максимальное количество процессов для фоновых задач проверки по требованию.

Чтобы изменить приоритет задачи проверки по требованию, выполните следующие действия:

1. Откройте окно **Свойства: Проверка по требованию**.

2. Установите или снимите флажок **Выполнять задачу в фоновом режиме**.

3. Нажмите на кнопку **OK**.

Настроенные параметры задачи будут сохранены и применены немедленно в выполняющейся задаче. Если задача не выполняется, измененные параметры будут применены при ее последующем запуске.

Регистрация выполнения задачи Проверка важных областей

По умолчанию статус защиты устройства отображается в панели результатов узла **Kaspersky Embedded Systems Security** и обновляется еженедельно после завершения задачи Проверка важных областей.

Время обновления статуса защиты устройства привязано к расписанию задачи проверки по требованию, в параметрах которой установлен флажок **Считать выполнение задачи проверкой важных областей**. По умолчанию флажок установлен только для задачи Проверка важных областей и недоступен для редактирования в этой задаче.

Вы можете выбрать задачу проверки по требованию, связанную со статусом защиты устройства, только в Kaspersky Security Center.

Настройка области проверки для задачи

Если вы изменили область проверки в задачах Проверка при старте операционной системы и Проверка важных областей, можно восстановить область проверки по умолчанию для этих задач, выполнив восстановление Kaspersky Embedded Systems Security (**Пуск** > **Программы** > **Kaspersky Embedded Systems Security** > **Изменение или удаление Kaspersky Embedded Systems Security**). В мастере установки выберите **Восстановление установленных компонентов** и нажмите на кнопку **Далее**. Затем установите флажок **Восстановить рекомендуемые параметры работы программы**.

Чтобы настроить область проверки для задачи проверки по требованию, выполните следующие действия:

1. Откройте окно **Свойства: Проверка по требованию**.
2. Выберите закладку **Область проверки**.
3. Чтобы включить элементы в область проверки:
   a. Откройте контекстное меню для списка областей проверки.
   b. В контекстном меню выберите пункт **Добавить область**.
   c. В открывшемся окне **Добавление в область проверки** выберите тип объектов, который вы хотите добавить:
      - **Предопределенная область**, чтобы добавить одну из стандартных областей на защищаемом устройстве. Затем в раскрывающемся списке выберите требуемую область проверки.
      - **Диск, папка или сетевой объект**, чтобы включить в область проверки отдельный диск, папку или сетевой объект. Затем выберите нужную область, нажав на кнопку **Обзор**.
      - **Файл**, чтобы включить в область проверки отдельный файл. Затем выберите нужную область, нажав на кнопку **Обзор**.

   Нельзя добавить объект в область проверки, если он уже добавлен в качестве исключения из области проверки.
4. Чтобы исключить отдельные узлы из области проверки, снимите флажки рядом с именами этих узлов или выполните следующие действия:
   a. Откройте контекстное меню области проверки по правой клавише мыши.
   b. В контекстном меню выберите пункт **Добавить исключение**.

c. В окне **Добавление исключения** выберите тип объектов, который вы хотите добавить в качестве исключения из области проверки, по аналогии с добавлением объекта в область проверки.

5. Чтобы изменить область проверки или исключение, в контекстном меню требуемой области проверки выберите пункт **Изменить область**.

6. Чтобы скрыть добавленную ранее область проверки или исключения из списка сетевых файловых ресурсов, в контекстном меню требуемой области выберите пункт **Удалить область**.

   Область проверки будет удалена из области действия задачи проверки по требованию при ее удалении из списка сетевых файловых ресурсов.

7. Нажмите на кнопку **OK**.

Окно параметров области проверки закроется. Настроенные параметры задачи будут сохранены.

Выбор стандартных уровней безопасности в задачах проверки по требованию

Для узлов, выбранных в списке файловых ресурсов защищаемого устройства, можно задать один из трех стандартных уровней безопасности: **Максимальное быстродействие**, **Рекомендуемый** и **Максимальная защита**.

Чтобы выбрать один из стандартных уровней безопасности, выполните следующие действия:

1. Откройте окно **Свойства: Проверка по требованию**.

2. Выберите закладку **Область проверки**.

3. В списке защищаемых устройств выберите элемент, включенный в область проверки, чтобы задать для него стандартный уровень безопасности.

4. Нажмите на кнопку **Настроить**.

   Откроется окно **Настройка проверки по требованию**.

5. На закладке **Уровень безопасности** выберите требуемый уровень безопасности.

   В окне отобразится список значений параметров безопасности, которые соответствуют выбранному вами уровню безопасности.

6. Нажмите на кнопку **OK**.

7. В окне **Свойства: Проверка по требованию** нажмите на кнопку **OK**.

   Настроенные параметры задачи будут сохранены и применены немедленно в выполняющейся задаче. Если задача не выполняется, измененные параметры будут применены при ее последующем запуске.

Настройка параметров безопасности вручную

По умолчанию в задачах проверки по требованию применяются единые параметры безопасности для всей области проверки.

Эти параметры соответствуют стандартному уровню безопасности **Рекомендуемый**.

Можно изменять значения параметров безопасности, заданные по умолчанию, настроив их как едиными для всей области проверки, так и различными для отдельных элементов в дереве или списке файловых ресурсов защищаемого устройства.

Чтобы настроить параметры безопасности вручную, выполните следующие действия:

1. Откройте окно **Свойства: Проверка по требованию**.
2. Выберите закладку **Область проверки**.
3. В списке областей проверки выберите элементы, для которых вы хотите настроить параметры безопасности.

   Стандартный шаблон параметров безопасности можно применить к выбранному узлу или элементу в области проверки.

4. Нажмите на кнопку **Настроить**.

   Откроется окно **Настройка проверки по требованию**.

5. На следующих закладках настройте параметры безопасности выбранного узла или элемента в соответствии с вашими требованиями:

   - **Общие**
   - **Действия**
   - **Производительность**
   - **Иерархическое хранилище**

6. Нажмите на кнопку **ОК** в окне **Настройка проверки по требованию**.
7. Нажмите на кнопку **ОК** в окне **Область проверки**.

Новые параметры области проверки будут сохранены.

Настройка общих параметров задачи

Чтобы настроить общие параметры задачи проверки по требованию, выполните следующие действия:

1. Откройте окно **Свойства: Проверка по требованию**.
2. Выберите закладку **Область проверки**.
3. Нажмите на кнопку **Настроить**.

   Откроется окно **Настройка проверки по требованию**.

4. Нажмите на кнопку **Настройка**.

5. На закладке **Общие** в блоке параметров **Проверка объектов** укажите типы объектов, которые вы хотите включить в область проверки:

   - **Объекты проверки**:
     - **Все объекты**
     - **Объекты, проверяемые по формату**
     - **Объекты, проверяемые по списку расширений, указанному в антивирусных базах**
     - **Объекты, проверяемые по указанному списку расширений**
   - **Вложенные папки**
   - **Вложенные файлы**
   - **Загрузочные секторы дисков и MBR**
   - **Альтернативные потоки NTFS**

6. В блоке параметров **Оптимизация** установите или снимите флажок **Проверка только новых и измененных файлов**.

   Для переключения между доступными вариантами при снятом флажке перейдите по ссылке **Все** / **Только новые** для каждого типа составных объектов.

7. В блоке параметров **Проверка составных объектов** укажите составные объекты, которые вы хотите включить в область проверки:

   - **Все** / **Только новые архивы**
   - **Все** / **Только новые SFX-архивы**
   - **Все** / **Только новые почтовые базы**
   - **Все** / **Только новые упакованные объекты**
   - **Все** / **Только новые файлы почтовых форматов**
   - **Все** / **Только новые вложенные OLE-объекты**

8. Нажмите на кнопку **OK**.

Новая конфигурация задачи будет сохранена.

Настройка действий

Чтобы настроить действия над зараженными и другими обнаруженными объектами во время выполнения задачи проверки по требованию, выполните следующие действия:

1. Откройте окно **Свойства: Проверка по требованию**.

2. Выберите закладку **Область проверки**.
3. Нажмите на кнопку **Настроить**.

   Откроется окно **Настройка проверки по требованию**.
4. Нажмите на кнопку **Настройка**.
5. Выберите закладку **Действия**.
6. Выберите действие над зараженными и другими обнаруживаемыми объектами:
   - **Только сообщать**
   - **Лечить**
   - **Лечить. Удалять, если лечение невозможно**
   - **Удалять**
   - **Выполнять рекомендуемое действие**
7. Выберите действие над возможно зараженными объектами:
   - **Только сообщать**
   - **Помещать на карантин**
   - **Удалять**
   - **Выполнять рекомендуемое действие**
8. Настройте действия над объектами в зависимости от типа обнаруженного объекта:
   a. Снимите или установите флажок **Выполнять действия в зависимости от типа обнаруженного объекта**.
   b. Нажмите на кнопку **Настройка**.
   c. В открывшемся окне выберите первичное действие и (на случай неудачного выполнения первичного действия) вторичное действие для каждого типа обнаруженного объекта.
   d. Нажмите на кнопку **OK**.
9. Выберите действие над неизлечимыми составными объектами: снимите или установите флажок **Полностью удалять составной файл при обнаружении вложенного объекта, если составной файл не может быть изменен программой**.
10. Нажмите на кнопку **OK**.

Новая конфигурация задачи будет сохранена.

Настройка производительности

Чтобы настроить производительность задачи проверки по требованию, выполните следующие действия:

1. Откройте окно **Свойства: Проверка по требованию**.
2. Выберите закладку **Область проверки**.
3. Нажмите на кнопку **Настроить**.

   Откроется окно **Настройка проверки по требованию**.
4. Нажмите на кнопку **Настройка**.
5. Выберите закладку **Производительность**.
6. В блоке **Исключения**:
   - Снимите или установите флажок **Исключать файлы**.
   - Снимите или установите флажок **Не обнаруживать**.
   - Нажмите на кнопку **Изменить** для каждого параметра, чтобы добавить исключения.
7. В блоке **Дополнительные параметры**:
   - **Останавливать проверку, если она длится более (сек.)**
   - **Не проверять составные объекты размером более (МБ)**
   - **Использовать технологию iSwift**
   - **Использовать технологию iChecker**
8. Нажмите на кнопку **OK**.

Новая конфигурация задачи будет сохранена.

Настройка проверки съемных дисков

Чтобы настроить проверку съемных дисков при их подключении к защищаемому устройству, выполните следующие действия:

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой вы хотите настроить задачу.
3. Выберите закладку **Политики**.
4. Откройте окно свойств политики двойным щелчком мыши на имени политики, которую вы хотите настроить.

   В открывшемся окне **Свойства: <Имя политики>** перейдите в раздел **Дополнительные возможности**.
5. Нажмите на кнопку **Настройка** в подразделе **Проверка съемных дисков**.

   Откроется окно **Проверка съемных дисков**.
6. В блоке **Параметры проверки при подключении** выполните следующие действия:

- Установите флажок **Проверять съемные диски при их подключении по USB**, если вы хотите, чтобы программа Kaspersky Embedded Systems Security автоматически выполняла проверку съемных дисков при их подключении.

- Если требуется, установите флажок **Проверять, если объем содержащихся на диске данных не превышает порог (МБ)** и укажите максимальное значение объема данных в поле справа.

- В раскрывающемся списке **Запускать проверку с уровнем безопасности** укажите уровень безопасности, в соответствии с которым требуется выполнять проверку съемных дисков.

7. Нажмите на кнопку **ОК**.

Настроенные параметры будут сохранены и применены.

Настройка задачи Мониторинг целостности файлов на основе эталона

Чтобы настроить групповую задачу Мониторинг целостности файлов на основе эталона, выполните следующие действия:

1. В дереве Консоли администрирования Kaspersky Security Center разверните узел **Управляемые устройства** и выберите группу администрирования, для которой вы хотите настроить задачи.

2. В панели результатов выбранной группы администрирования выберите закладку **Задачи**.

3. В списке ранее созданных групповых задач выберите задачу, параметры которой хотите настроить. Откройте окно **Свойства: <Название задачи>** одним из следующих способов:

   - Выберите название задачи в списке созданных задач двойным щелчком мыши.

   - Выделите название задачи в списке созданных задач и перейдите по ссылке **Настроить задачу**.

   - Откройте контекстное меню задачи в списке созданных задач и выберите пункт **Свойства**.

   В разделе **Уведомления** настройте параметры уведомлений о событиях задачи. Подробная информация о настройке параметров в этом разделе приведена в *Справке Kaspersky Security Center.*

4. В разделе **Область мониторинга** выполните следующие действия:

   a. Чтобы добавить папку в область задачи Мониторинг целостности файлов на основе эталона:

      1. Нажмите на кнопку **Добавить**.

         Откроется окно **Область проверки**.

      2. Установите или снимите флажок **Проверять эту область**.

      3. Нажмите на кнопку **Обзор**, чтобы указать папку, которую вы хотите включить в область задачи Мониторинг целостности файлов на основе эталона.

      4. Установите флажок **Также проверять подпапки**, чтобы включить все вложенные папки в область задачи Мониторинг целостности файлов на основе эталона.

   b. Чтобы добавить или исключить добавленную ранее папку из области задачи Мониторинг целостности файлов на основе эталона, снимите или установите флажок слева от пути к папке в таблице **Область мониторинга**.

c. Чтобы удалить папку, добавленную в область задачи Мониторинг целостности файлов на основе эталона, выберите папку в таблице **Область мониторинга** и нажмите на кнопку **Удалить**.

5. В разделе **Расписание** настройте параметры расписания задачи (вы можете настраивать расписание всех задач, кроме задачи Откат обновления баз программы).

6. В разделе **Учетная запись** укажите учетную запись, с правами которой будет выполняться задача.

7. Если требуется, в разделе **Исключения** из области действия задачи укажите объекты, которые хотите исключить из области действия задачи.

   Подробная информация о настройке параметров в этом разделе приведена в *Справке Kaspersky Security Center*.

8. В окне **Свойства: <Название задачи>** нажмите на кнопку **ОК**.

   Настроенные параметры групповых задач будут сохранены.

Управление задачами проверки по требованию с помощью Консоли программы

В этом разделе описана навигация в интерфейсе Консоли программы и настройка параметров задачи на защищаемом устройстве.

Навигация

В этом разделе описан переход к требуемым параметрам задачи с помощью интерфейса.

Переход к параметрам задачи проверки по требованию

Чтобы перейти к общим параметрам задачи проверки по требованию в Консоли программы, выполните следующие действия:

1. В дереве Консоли программы разверните узел **Проверка по требованию**.

2. Выберите вложенный узел, соответствующий задаче, которую вы хотите настроить.

3. В панели результатов вложенного узла перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи**.

Переход к параметрам области действия задачи проверки по требованию

Чтобы перейти к параметрам области проверки в Консоли программы, выполните следующие действия:

1. В дереве Консоли программы разверните узел **Проверка по требованию**.
2. Выберите вложенный узел, соответствующий задаче проверки по требованию, параметры которой вы хотите настроить.
3. В панели результатов выбранного узла перейдите по ссылке **Настроить область проверки**.

   Откроется окно **Настройка области проверки**.

Создание и настройка задачи проверки по требованию

Вы можете создавать пользовательские задачи для отдельного защищаемого устройства в узле **Проверка по требованию**. В других функциональных компонентах Kaspersky Embedded Systems Security создание пользовательских задач не предусмотрено.

Чтобы создать и настроить задачу проверки по требованию, выполните следующие действия:

1. В дереве Консоли программы откройте контекстное меню узла **Проверка по требованию**.
2. Выберите пункт **Добавить задачу**.

   Откроется окно **Добавить задачу**.
3. Настройте следующие параметры задачи:

   - **Имя** – название задачи, содержащее не более 100 символов. Допускаются любые символы, кроме **" * < > & \ : |**.

     Вы не можете сохранить новую задачу или перейти к настройке параметров новой задачи на закладках **Расписание**, **Дополнительно** и **Запуск с правами**, если не задано название задачи.

   - **Описание** – дополнительная информация о задаче, не более 2000 символов. Эта информация отображается в окне свойств задачи.
   - **Использовать эвристический анализатор**.
   - **Выполнять задачу в фоновом режиме**.
   - **Применять доверенную зону**.
   - **Считать выполнение задачи проверкой важных областей**.
   - **Использовать KSN для проверки**.
4. Настройте расписание запуска задачи на закладках **Расписание** и **Дополнительно**.
5. На закладке **Запуск с правами** настройте параметры запуска задачи с использованием прав учетной записи.
6. В окне **Добавить задачу** нажмите на кнопку **OK**.

Новая пользовательская задача проверки по требованию будет создана. Узел с названием новой задачи будет отображен в дереве Консоли программы. Операция регистрируется в журнале системного аудита.

7. Если требуется, в панели результатов выбранного узла выберите **Настроить область проверки**.

   Откроется окно **Настройка области проверки**.

8. В дереве или в списке файловых ресурсов защищаемого устройства выберите узлы или элементы, которые вы хотите включить в область проверки.

9. Выберите один из стандартных уровней безопасности или настройте параметры проверки вручную.

10. Нажмите на кнопку **Сохранить** в окне **Настройка области проверки**.

Настроенные параметры будут применены при последующем запуске задачи.

Область проверки в задачах проверки по требованию

Этот раздел содержит информацию о формировании и использовании области проверки в задачах проверки по требованию.

Настройка отображения сетевых файловых ресурсов

Чтобы выбрать отображение сетевых файловых ресурсов при настройке параметров области проверки, выполните следующие действия:

1. Откройте окно **Настройка области проверки**.

2. В раскрывающемся списке в левом верхнем углу окна выберите один из следующих вариантов:

   - Выберите **Показывать в виде дерева**, чтобы сетевые файловые ресурсы отображались в виде дерева.
   - Выберите **Показывать в виде списка**, чтобы сетевые файловые ресурсы отображались в виде списка.

   По умолчанию сетевые файловые ресурсы защищаемого устройства отображаются в виде списка.

3. Нажмите на кнопку **Сохранить**.

Формирование области проверки

Если вы управляете Kaspersky Embedded Systems Security на защищаемом устройстве удаленно, с помощью Консоли программы, установленной на рабочем месте администратора, вы должны входить в группу администраторов на защищаемом устройстве, чтобы просматривать папки на нем.

Названия параметров могут отличаться в разных операционных системах Windows.

Если вы изменили область проверки в задачах Проверка при старте операционной системы и Проверка важных областей, можно восстановить область проверки по умолчанию для этих задач, выполнив восстановление Kaspersky Embedded Systems Security (**Пуск** > **Программы** > **Kaspersky Embedded Systems Security** > **Изменение или удаление Kaspersky Embedded Systems Security**). В мастере установки выберите **Восстановление установленных компонентов** и нажмите на кнопку **Далее**. Затем установите флажок **Восстановить рекомендуемые параметры работы программы**.

Процедура формирования области проверки в задачах проверки по требованию зависит от выбранного типа отображения сетевых файловых ресурсов. Сетевые файловые ресурсы могут отображаться в виде дерева или в виде списка (по умолчанию).

Чтобы сформировать область проверки с помощью дерева сетевых файловых ресурсов, выполните следующие действия:

1. Откройте окно **Настройка области проверки**.
2. В левой части окна разверните дерево сетевых файловых ресурсов, чтобы отобразить все узлы.
3. Выполните следующие действия:
   - Чтобы исключить отдельные узлы из области проверки, снимите флажки рядом с именами этих узлов.
   - Чтобы включить отдельные узлы в область проверки, снимите флажок **Мой компьютер** и выполните следующие действия:
     - Если вы хотите включить в область проверки все диски определенного типа, установите флажок рядом с названием нужного типа дисков (например, чтобы включить все съемные диски защищаемого устройства, установите флажок **Съемные диски**).
     - Если вы хотите включить в область проверки отдельный диск определенного типа, разверните узел, который содержит диски этого типа, и установите флажок рядом с именем требуемого диска. Например, чтобы выбрать съемный диск **F:**, разверните узел **Съемные диски** и установите флажок для диска **F:**.
     - Если вы хотите включить в область защиты только отдельную папку или отдельный файл на диске, установите флажок рядом с именем этой папки или этого файла.
4. Нажмите на кнопку **Сохранить**.

Окно **Настройка области проверки** будет закрыто. Настроенные параметры задачи будут сохранены.

Чтобы сформировать область проверки с помощью списка сетевых файловых ресурсов, выполните следующие действия:

1. Откройте окно **Настройка области проверки**.
2. Чтобы включить отдельные узлы в область проверки, снимите флажок **Мой компьютер** и выполните следующие действия:
   a. Откройте контекстное меню области проверки по правой клавише мыши.
   b. В контекстном меню выберите пункт **Добавить область проверки**.
   c. В открывшемся окне **Добавление области проверки** выберите тип объектов, который вы хотите добавить:

- **Предопределенная область**, чтобы добавить одну из стандартных областей на защищаемом устройстве. Затем в раскрывающемся списке выберите требуемую область проверки.
- **Диск, папка или сетевой объект**, чтобы включить в область проверки отдельный диск, папку или сетевой объект. Затем выберите нужную область, нажав на кнопку **Обзор**.
- **Файл**, чтобы включить в область проверки отдельный файл. Затем выберите нужную область, нажав на кнопку **Обзор**.

Нельзя добавить объект в область проверки, если он уже добавлен в качестве исключения из области проверки.

3. Чтобы исключить отдельные узлы из области проверки, снимите флажки рядом с именами этих узлов или выполните следующие действия:
   a. Откройте контекстное меню области проверки по правой клавише мыши.
   b. В контекстном меню выберите пункт **Добавить исключение**.
   c. В окне **Добавление исключения** выберите тип объектов, который вы хотите добавить в качестве исключения из области проверки, по аналогии с добавлением объекта в область проверки.
4. Чтобы изменить добавленную область проверки или исключение, в контекстном меню нужной области проверки выберите пункт **Изменить область**.
5. Чтобы скрыть добавленную ранее область проверки или исключения из списка сетевых файловых ресурсов, в контекстном меню требуемой области выберите пункт **Удалить из списка**.

Область проверки будет удалена из области действия задачи проверки по требованию при ее удалении из списка сетевых файловых ресурсов.

6. Нажмите на кнопку **Сохранить**.

Окно **Настройка области проверки** будет закрыто. Настроенные параметры задачи будут сохранены.

Включение в область проверки сетевых объектов

Вы можете включать в область проверки сетевые диски, папки и файлы, указывая сетевые пути к ним в формате UNC (Universal Naming Convention).

Вы можете проверять сетевые папки при работе под системной учетной записью.

Чтобы включить в область проверки сетевой объект, выполните следующие действия:

1. Откройте окно **Настройка области проверки**.
2. В раскрывающемся списке в левом верхнем углу окна выберите пункт **Показывать в виде дерева**.
3. В контекстном меню узла **Сетевое окружение** выполните следующие действия:

- Выберите пункт **Добавить сетевую папку**, если вы хотите добавить сетевую папку в область проверки.
- Выберите пункт **Добавить сетевой файл**, если вы хотите добавить сетевой файл в область проверки.

4. Введите путь к сетевой папке или файлу в формате UNC (Universal Naming Convention) и нажмите на клавишу **ENTER**.
5. Установите флажок рядом с именем добавленного сетевого объекта, чтобы включить его в область проверки.
6. Если требуется, измените параметры безопасности для добавленного сетевого объекта.
7. Нажмите на кнопку **Сохранить**.

Настроенные изменения параметров задачи будут сохранены.

Создание виртуальной области проверки

Можно включать в область проверки виртуальные диски, папки и файлы, таким образом создавая виртуальную область проверки.

Вы можете включить в область проверки отдельные виртуальные диски, папки или файлы, только если область проверки отображается в виде дерева файловых ресурсов.

Чтобы включить в область проверки виртуальный диск, выполните следующие действия:

1. Откройте окно **Настройка области проверки**.
2. В раскрывающемся списке в левом верхнем углу окна выберите пункт **Показывать в виде дерева**.
3. В дереве файловых ресурсов защищаемого устройства откройте контекстное меню узла **Виртуальные диски**, выберите пункт **Добавить виртуальный диск** и в списке доступных имен выберите имя виртуального диска.
4. Установите флажок рядом с добавленным диском, чтобы включить диск в область проверки.
5. Нажмите на кнопку **Сохранить**.

Настроенные изменения параметров задачи будут сохранены.

Чтобы включить в область проверки виртуальную папку или виртуальный файл, выполните следующие действия:

1. Откройте окно **Настройка области проверки**.
2. В раскрывающемся списке в левом верхнем углу окна выберите пункт **Показывать в виде дерева**.
3. В дереве файловых ресурсов защищаемого устройства откройте контекстное меню узла, в который вы хотите добавить папку или файл, и выберите один из следующих вариантов:
   - **Добавить виртуальную папку**, если вы хотите добавить виртуальную папку в область проверки.
   - **Добавить виртуальный файл**, если вы хотите добавить виртуальный файл в область проверки.

4. В поле ввода задайте имя для папки или файла.

5. В строке с именем папки или файла установите флажок, чтобы включить папку или файл в область проверки.

6. Нажмите на кнопку **Сохранить**.

Настроенные изменения параметров задачи будут сохранены.

Настройка параметров безопасности

По умолчанию в задачах проверки по требованию применяются единые параметры безопасности для всей области проверки.

Эти параметры соответствуют стандартному уровню безопасности **Рекомендуемый**.

Можно изменять значения параметров безопасности, заданные по умолчанию, настроив их как едиными для всей области проверки, так и различными для отдельных элементов в дереве или списке файловых ресурсов защищаемого устройства.

При работе с деревом сетевых файловых ресурсов параметры безопасности, настроенные для выбранного родительского узла, автоматически применяются для всех вложенных узлов. Параметры безопасности родительского узла не применяются к вложенному узлу, который настраивается отдельно.

Чтобы настроить параметры безопасности вручную, выполните следующие действия:

1. Откройте окно **Настройка области проверки**.

2. В левой части окна выберите узел или элемент, параметры безопасности которого вы хотите настроить.

   Стандартный шаблон параметров безопасности можно применить к выбранному узлу или элементу в области проверки.

   В левой части окна можно выбрать тип отображения сетевых файловых ресурсов, создать область проверки и создать виртуальную область проверки.

3. В правой части окна выполните одно из следующих действий:

   - На закладке **Уровень безопасности** выберите требуемый уровень безопасности.

   - На следующих закладках настройте параметры безопасности выбранного узла или элемента в соответствии с вашими требованиями:

     - **Общие**

     - **Действия**

     - **Производительность**

     - **Иерархическое хранилище**

4. Нажмите на кнопку **Сохранить** в окне **Настройка области проверки**.

Новые параметры области проверки будут сохранены.

Выбор стандартных уровней безопасности в задачах проверки по требованию

Для выбранных в дереве или списке файловых ресурсов защищаемого устройства узлов можно задать один из следующих стандартных уровней безопасности: **Максимальное быстродействие**, **Рекомендуемый** и **Максимальная защита**.

Чтобы выбрать один из стандартных уровней безопасности, выполните следующие действия:

1. Откройте окно **Настройка области проверки**.
2. В дереве или в списке сетевых файловых ресурсов защищаемого устройства выберите узел или элемент, для которого вы хотите задать стандартный уровень безопасности.
3. Убедитесь, что выбранный узел или элемент включен в область проверки.
4. В правой части окна на закладке **Уровень безопасности** выберите требуемый уровень безопасности.

   В окне отобразится список значений параметров безопасности, соответствующих выбранному уровню безопасности.
5. Нажмите на кнопку **Сохранить**.

   Параметры задачи будут сохранены и применены немедленно в выполняющейся задаче. Если задача не выполняется, измененные параметры будут применены при ее следующем запуске.

Настройка общих параметров задачи

Чтобы настроить общие параметры безопасности задачи проверки по требованию, выполните следующие действия:

1. Откройте окно **Настройка области проверки**.
2. Выберите закладку **Общие**.
3. В блоке параметров **Проверка объектов** укажите типы объектов, которые вы хотите включить в область проверки:
   - **Объекты проверки**:
     - **Все объекты**
     - **Объекты, проверяемые по формату**
     - **Объекты, проверяемые по списку расширений, указанному в антивирусных базах**
     - **Объекты, проверяемые по указанному списку расширений**
   - **Загрузочные секторы дисков и MBR**
   - **Альтернативные потоки NTFS**

4. В блоке параметров **Оптимизация** установите или снимите флажок **Проверка только новых и измененных файлов**.

   Для переключения между доступными вариантами при снятом флажке перейдите по ссылке **Все** / **Только новые** для каждого типа составных объектов.

5. В блоке параметров **Проверка составных объектов** укажите составные объекты, которые вы хотите включить в область проверки:

   - **Все** / **Только новые архивы**
   - **Все** / **Только новые SFX-архивы**
   - **Все** / **Только новые почтовые базы**
   - **Все** / **Только новые упакованные объекты**
   - **Все** / **Только новые файлы почтовых форматов**
   - **Все** / **Только новые вложенные OLE-объекты**

6. Нажмите на кнопку **Сохранить**.

Новая конфигурация задачи будет сохранена.

Настройка действий

Чтобы настроить действия, которые задача проверки по требованию выполняет над зараженными и другими обнаруженными объектами, выполните следующие действия:

1. Откройте окно **Настройка области проверки**.
2. Выберите закладку **Действия**.
3. Выберите действие над зараженными и другими обнаруживаемыми объектами:

   - **Только сообщать**
   - **Лечить**
   - **Лечить. Удалять, если лечение невозможно**
   - **Удалять**
   - **Выполнять рекомендуемое действие**

4. Выберите действие над возможно зараженными объектами:

   - **Только сообщать**
   - **Помещать на карантин**
   - **Удалять**

- **Выполнять рекомендуемое действие**

5. Настройте действия над объектами в зависимости от типа обнаруженного объекта:

   a. Снимите или установите флажок **Выполнять действия в зависимости от типа обнаруженного объекта**.

   b. Нажмите на кнопку **Настройка**.

   c. В открывшемся окне выберите первичное действие и (на случай неудачного выполнения первичного действия) вторичное действие для каждого типа обнаруженного объекта.

   d. Нажмите на кнопку **ОК**.

6. Выберите действие над неизлечимыми составными объектами: снимите или установите флажок **Полностью удалять составной файл при обнаружении вложенного объекта, если составной файл не может быть изменен программой**.

7. Нажмите на кнопку **Сохранить**.

Новая конфигурация задачи будет сохранена.

Настройка производительности

Чтобы настроить производительность задачи проверки по требованию, выполните следующие действия:

1. Откройте окно **Настройка области проверки**.

2. Выберите закладку **Производительность**.

3. В блоке **Исключения**:

   - Снимите или установите флажок **Исключать файлы**.
   - Снимите или установите флажок **Не обнаруживать**.
   - Нажмите на кнопку **Изменить** для каждого параметра, чтобы добавить исключения.

4. В блоке **Дополнительные параметры**:

   - **Останавливать проверку, если она длится более (сек.)**
   - **Не проверять составные объекты размером более (МБ)**
   - **Использовать технологию iSwift**
   - **Использовать технологию iChecker**

5. Нажмите на кнопку **Сохранить**.

Новая конфигурация задачи будет сохранена.

Настройка иерархического хранилища

Чтобы настроить действия, которые задача проверки по требованию выполняет над зараженными и другими обнаруженными объектами, выполните следующие действия:

1. Откройте окно **Настройка области проверки**.
2. Выберите закладку **Иерархическое хранилище**.
3. Выберите одно из следующих действий над файлами:
   - **Не проверять**
   - **Проверять только резидентную часть файла**
   - **Проверять файл полностью**

     Если выбрано это действие, доступны следующие параметры проверки:

     - Снимите или установите флажок **Только если обращение к файлу производилось в указанный период (сут)** и укажите количество дней.
     - Снимите или установите флажок **Не копировать файл на локальный жесткий диск, если возможно**.
4. Нажмите на кнопку **Сохранить**.

Новая конфигурация задачи будет сохранена.

Проверка съемных дисков

Чтобы настроить проверку съемных дисков при их подключении к защищаемому устройству в Консоли программы, выполните следующие действия:

1. В дереве Консоли программы откройте контекстное меню узла **Kaspersky Embedded Systems Security** и выберите пункт **Настроить проверку съемных дисков**.

   Откроется окно **Проверка съемных дисков**.
2. В блоке **Параметры проверки при подключении** выполните следующие действия:
   - Установите флажок **Проверять съемные диски при их подключении по USB**, если вы хотите, чтобы программа Kaspersky Embedded Systems Security автоматически выполняла проверку съемных дисков при их подключении.
   - Если требуется, установите флажок **Проверять, если объем содержащихся на диске данных не превышает порог (МБ)** и укажите максимальное значение объема данных в поле справа.
   - В раскрывающемся списке **Запускать проверку с уровнем безопасности** укажите уровень безопасности, в соответствии с которым требуется выполнять проверку съемных дисков.
3. Нажмите на кнопку **ОК**.

Настроенные параметры будут сохранены и применены.

Статистика задач проверки по требованию

Пока выполняется задача проверки по требованию, вы можете просматривать информацию о количестве объектов, которые программа Kaspersky Embedded Systems Security обработала с момента запуска задачи.

Эта информация будет доступна, даже если вы приостановите задачу. Вы можете просмотреть статистику задачи в журнале выполнения задачи.

Чтобы просмотреть статистику задачи проверки по требованию, выполните следующие действия:

1. В дереве Консоли программы разверните узел **Проверка по требованию**.
2. Выберите задачу проверки по требованию, статистику которой вы хотите просмотреть.

   В панели результатов выбранного узла в блоке **Статистика** отобразится статистика задачи.

В таблице ниже приведена информация об объектах, которые программа Kaspersky Embedded Systems Security обработала с момента запуска задачи.

Статистика задач проверки по требованию

Поле	Описание
Обнаружено	Количество объектов, которые обнаружила программа Kaspersky Embedded Systems Security. Например, если программа Kaspersky Embedded Systems Security обнаружила один вредоносный объект в пяти файлах, значение в этом поле увеличится на единицу.
Зараженных и других обнаруживаемых объектов	Количество объектов, которые программа Kaspersky Embedded Systems Security признала зараженными, или количество обнаруженных объектов, которые не были исключены из области действия задач проверки по требованию и были определены как легальные программы, которые могут быть использованы злоумышленниками для нанесения вреда устройству или персональным данным.
Возможно зараженных объектов	Количество объектов, которые программа Kaspersky Embedded Systems Security признала возможно зараженными.
Объектов не вылечено	Количество объектов, которые программа Kaspersky Embedded Systems Security не вылечила по следующим причинам: • Тип обнаруженного объекта не предполагает лечения. • При лечении возникла ошибка.
Объектов не помещено на карантин	Количество объектов, которые программе Kaspersky Embedded Systems Security не удалось поместить на карантин, например, из-за отсутствия свободного места на диске.
Объектов не удалено	Количество объектов, которые программе Kaspersky Embedded Systems Security не удалось удалить, например, если доступ к объекту был заблокирован другой программой.
Объектов не проверено	Количество объектов в области защиты, которые программе Kaspersky Embedded Systems Security не удалось проверить, например, если доступ к объекту был заблокирован другой программой.
Объектов, не помещенных в резервное хранилище	Количество объектов, копии которых программе Kaspersky Embedded Systems Security не удалось сохранить в резервном хранилище, например, из-за отсутствия свободного места на диске.
Ошибок обработки	Количество объектов, во время обработки которых возникла ошибка задачи.

Вылечено объектов	Количество объектов, которые вылечила программа Kaspersky Embedded Systems Security.
Помещено на карантин	Количество объектов, которые программа Kaspersky Embedded Systems Security поместила на карантин.
Помещено в резервное хранилище	Количество объектов, копии которых программа Kaspersky Embedded Systems Security сохранила в резервном хранилище.
Удалено объектов	Количество объектов, которые удалила программа Kaspersky Embedded Systems Security.
Защищенных паролем объектов	Количество объектов (например, архивов), которые программа Kaspersky Embedded Systems Security пропустила, так как эти объекты защищены паролем.
Поврежденных объектов	Количество объектов, которые программа Kaspersky Embedded Systems Security пропустила, так как их формат искажен.
Обработано объектов	Общее количество объектов, которые обработала программа Kaspersky Embedded Systems Security.

Вы также можете посмотреть статистику задачи проверки по требованию в журнале выполнения выбранной задачи по ссылке **Открыть журнал выполнения** в блоке **Управление** панели результатов.

По завершении выполнения задачи рекомендуется вручную обработать события в журнале выполнения задачи на закладке **События**.

Создание и настройка задачи Мониторинг целостности файлов на основе эталона

Чтобы создать или настроить задачу Мониторинг целостности файлов на основе эталона, выполните следующие действия:

1. В дереве Консоли программы откройте контекстное меню узла **Диагностика системы**.
2. Выберите пункт **Создать задачу мониторинга целостности файлов**.

   Откроется окно **Добавить задачу**.
3. В раскрывающемся списке **Алгоритм расчета контрольных сумм** выберите один из следующих вариантов:
   - **MD5**
   - **SHA256**
4. В таблице **Области проверки** выполните следующие действия:
   a. Чтобы добавить файл или папку в область задачи Мониторинг целостности файлов на основе эталона:
      1. Нажмите на кнопку **Добавить**.

         Откроется окно **Область проверки**.

2. Установите или снимите флажок **Проверять эту область**.

3. Нажмите на кнопку **Обзор**, чтобы указать файл или папку, которую вы хотите включить в область задачи Мониторинг целостности файлов на основе эталона.

4. Установите флажок **Также проверять подпапки**, чтобы включить все вложенные папки в область задачи Мониторинг целостности файлов на основе эталона.

5. Нажмите на кнопку **ОК**.

b. Чтобы поменять файл или папку, добавленную ранее в область задачи Мониторинг целостности файлов на основе эталона:

1. Нажмите на кнопку **Изменить**.

   Откроется окно **Область проверки**.

2. Установите или снимите флажок **Проверять эту область**.

3. Нажмите на кнопку **Обзор**, чтобы указать файл или папку, которую вы хотите включить в область задачи Мониторинг целостности файлов на основе эталона.

4. Установите или снимите флажок **Также проверять подпапки**, чтобы включить или исключить все вложенные папки из области задачи Мониторинг целостности файлов на основе эталона.

5. Нажмите на кнопку **ОК**.

c. Чтобы удалить файл или папку, добавленную в область задачи Мониторинг целостности файлов на основе эталона, выберите этот файл или папку в таблице **Области проверки** и нажмите на кнопку **Удалить**.

5. Настройте расписание запуска задачи на закладках **Расписание** и **Дополнительно**.

6. На закладке **Запуск с правами** настройте параметры запуска задачи с использованием прав учетной записи.

7. В окне **Добавить задачу** нажмите на кнопку **ОК**.

   Будет создана пользовательская задача Мониторинг целостности файлов на основе эталона. Узел с названием новой задачи будет отображен в дереве Консоли программы. Операция регистрируется в журнале системного аудита.

Чтобы просмотреть параметры задачи Мониторинг целостности файлов на основе эталона, выполните следующие действия:

1. В дереве Консоли программы разверните узел **Диагностика системы**.

2. Выберите вложенный узел, соответствующий задаче, которую вы хотите настроить.

3. В панели результатов вложенного узла перейдите по ссылке **Свойства**.

   Откроется окно **Параметры задачи**.

Управление задачами проверки по требованию с помощью Веб-плагина

В этом разделе описана навигация в интерфейсе Веб-плагина для защищаемых устройств в сети.

Переход к мастеру создания задачи проверки по требованию

Чтобы создать локальную задачу проверки по требованию, выполните следующие действия:

1. В главном окне веб-консоли выберите **Устройства** → **Управляемые устройства**.
2. Перейдите на закладку **Группы** и выберите группу администрирования, к которой принадлежит защищаемое устройство.
3. Выберите название защищаемого устройства.
4. В открывшемся окне **<Имя устройства>** выберите закладку **Задачи**.
5. Нажмите на кнопку **Добавить**.

   Откроется окно **Мастер создания задачи**.
6. В раскрывающемся списке **Программы** выберите **Kaspersky Embedded Systems Security**.
7. В раскрывающемся списке **Тип задачи** выберите задачу **Проверка по требованию**.
8. Нажмите на кнопку **Далее**.

Настройте параметры задачи в соответствии с вашими требованиями.

Чтобы создать групповую задачу проверки по требованию, выполните следующие действия:

1. В главном окне веб-консоли выберите **Устройства** → **Задачи**.
2. Перейдите на закладку **Группы** и выберите группу администрирования, для которой требуется создать задачу.
3. Нажмите на кнопку **Добавить**.

   Откроется окно **Мастер создания задачи**.
4. В раскрывающемся списке **Программы** выберите **Kaspersky Embedded Systems Security**.
5. В раскрывающемся списке **Тип задачи** выберите задачу **Проверка по требованию**.
6. Нажмите на кнопку **Далее**.

Настройте параметры задачи в соответствии с вашими требованиями.

Чтобы создать задачу проверки по требованию для произвольной группы, выполните следующие действия:

1. В главном окне веб-консоли выберите **Устройства** → **Выборки устройств**.
2. Выберите выборку устройств, для которой требуется создать задачу.
3. Нажмите на кнопку **Запустить**.
4. В окне **Результаты выборки** выберите устройства, для которых требуется создать задачу.

5. Нажмите на кнопку **Создать задачу**.
6. В раскрывающемся списке **Программы** выберите **Kaspersky Embedded Systems Security**.
7. В раскрывающемся списке **Тип задачи** выберите задачу **Проверка по требованию**.
8. Нажмите на кнопку **Далее**.

Настройте параметры задачи в соответствии с вашими требованиями.

Чтобы настроить задачу проверки по требованию, выполните следующие действия:

1. В главном окне веб-консоли выберите **Устройства** → **Задачи**.
2. Щелкните по названию задачи в списке задач Kaspersky Security Center.

Откроется окно **<Название задачи>**.

Переход к свойствам задачи проверки по требованию

Чтобы перейти к свойствам программы для задачи проверки по требованию для отдельного защищаемого устройства, выполните следующие действия:

1. В главном окне веб-консоли выберите **Устройства** → **Управляемые устройства**.
2. Перейдите на закладку **Группы** и выберите группу администрирования, к которой принадлежит защищаемое устройство.
3. Выберите название защищаемого устройства.
4. В открывшемся окне **<Имя устройства>** выберите закладку **Задачи**.
5. В списке задач, созданных для устройства, выберите созданную задачу проверки по требованию.
6. Перейдите на закладку **Параметры программы**.

Настройте параметры задачи в соответствии с вашими требованиями.

Доверенная зона

Этот раздел содержит информацию о доверенной зоне Kaspersky Embedded Systems Security, а также инструкции по добавлению объектов в доверенную зону при выполнении задач.

О доверенной зоне

Доверенная зона - это список исключений из области защиты или проверки, который вы можете сформировать и применять в задачах проверки по требованию и в задаче Постоянная защита файлов.

Если при установке Kaspersky Embedded Systems Security вы установили флажки **Добавить к исключениям файлы, рекомендованные Microsoft** и **Добавить к исключениям файлы, рекомендованные "Лабораторией Касперского"**, Kaspersky Embedded Systems Security добавляет файлы, рекомендованные Microsoft и "Лабораторией Касперского", в доверенную зону для задач постоянной защиты компьютера.

Вы можете формировать доверенную зону Kaspersky Embedded Systems Security по следующим правилам:

- Доверенные процессы. В доверенную зону помещаются объекты, чувствительные к перехватам файловых операций процессами программы.
- Операции резервного копирования. В доверенную зону помещаются объекты, доступ к которым выполняется при операциях резервного копирования жестких дисков на внешние устройства.
- Исключения. В доверенную зону помещаются объекты, указанные по их местоположению и / или обнаруженному в них объекту.

Вы можете применить доверенную зону в задаче Постоянная защита файлов, в создаваемых пользовательских задачах проверки по требованию, а также во всех системных задачах проверки по требованию, кроме задачи Проверка объектов на карантине.

По умолчанию доверенная зона применяется в задаче Постоянная защита файлов и в задачах проверки по требованию.

Вы можете экспортировать список правил формирования доверенной зоны в конфигурационный XML-файл, чтобы затем импортировать его в Kaspersky Embedded Systems Security на другом защищаемом устройстве.

Доверенные процессы

Применяется в задачах Постоянная защита файлов и Защита трафика.

Некоторые программы на защищаемом устройстве могут работать нестабильно, если файлы, к которым они обращаются, перехватываются Kaspersky Embedded Systems Security. К таким программам относятся, например, системные программы домен-контроллеров.

Чтобы не нарушать работу таких программ, вы можете выключить защиту файлов, к которым обращаются выполняющиеся процессы этих программ, сформировав в доверенной зоне список доверенных процессов.

Корпорация Microsoft рекомендует исключать из постоянной защиты некоторые файлы операционной системы Microsoft Windows и файлы программ корпорации Microsoft как неподверженные заражению. Названия некоторых из них приведены на веб-сайте Microsoft (код статьи: KB822158).

Вы можете включать и выключать применение доверенных процессов в доверенной зоне.

Если исполняемый файл изменяется, например, в результате обновления, Kaspersky Embedded Systems Security исключает его из списка доверенных процессов.

Программа не использует путь к файлу на защищаемом устройстве для идентификации процесса как доверенного. Путь к файлу на защищаемом устройстве применяется только для поиска файла и расчета его контрольной суммы, а также для информирования пользователя об источнике исполняемого файла.

Операции резервного копирования

Применяется в задачах постоянной защиты компьютера.

На время резервного копирования данных, хранящихся на жестких дисках, на внешние устройства можно выключить защиту объектов, доступ к которым осуществляется при операциях резервного копирования. Kaspersky Embedded Systems Security будет проверять объекты, которые программа резервного копирования открывает на чтение с признаком FILE_FLAG_BACKUP_SEMANTICS.

Исключения

Применяется в задачах постоянной защиты файлов и проверки по требованию.

Вы можете выбрать задачи, в которых вы хотите применять каждое исключение, добавленное в доверенную зону. Также вы можете исключать объекты из проверки в параметрах уровня безопасности каждой задачи Kaspersky Embedded Systems Security по отдельности.

Вы можете добавлять в доверенную зону исключения по их расположению на защищаемом устройстве, по имени или маске имени обнаруженного объекта или использовать оба параметра.

На основании исключения Kaspersky Embedded Systems Security может пропускать в указанных задачах объекты согласно следующим параметрам:

- указанные объекты, обнаруживаемые по имени или маске имени в указанных областях защищаемого устройства;
- все обнаруживаемые объекты в указанных областях защищаемого устройства;
- указанные объекты, обнаруживаемые по имени или маске имени во всей области защиты или проверки.

Управление доверенной зоной с помощью Плагина управления

В этом разделе описана навигация в интерфейсе Плагина управления и настройка доверенной зоны для одного или всех защищаемых устройств в сети.

Навигация

В этом разделе описан переход к требуемым параметрам задачи с помощью интерфейса.

Переход к параметрам политики для доверенной зоны

Чтобы перейти к доверенной зоне в политике Kaspersky Security Center, выполните следующие действия:

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой вы хотите настроить задачу.
3. Выберите закладку **Политики**.
4. Откройте окно свойств политики двойным щелчком мыши на имени политики, которую вы хотите настроить.
5. В открывшемся окне **Свойства: <Имя политики>** перейдите в раздел **Дополнительные возможности**.
6. Нажмите на кнопку **Настройка** в подразделе **Доверенная зона**.

   Откроется окно **Доверенная зона**.

Настройте доверенную зону в соответствии с вашими требованиями.

Если защищаемое устройство работает под управлением активной политики Kaspersky Security Center и в этой политике запрещено изменение параметров программы, эти параметры недоступны для изменения в Консоли программы.

Переход к окну параметров доверенной зоны

Чтобы настроить доверенную зону в окне свойств программы, выполните следующие действия:

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой вы хотите настроить задачу.
3. Выберите закладку **Устройства**.
4. Откройте окно **Свойства: <Имя защищаемого устройства>** одним из следующих способов:
   - двойным щелчком мыши на имени защищаемого устройства;
   - выбрав пункт **Свойства** в контекстном меню защищаемого устройства.

   Откроется окно **Свойства: <Имя защищаемого устройства>**.
5. В разделе **Программы** выберите **Kaspersky Embedded Systems Security**.
6. Нажмите на кнопку **Свойства**.

   Откроется окно **Параметры программы Kaspersky Embedded Systems Security**.

7. Выберите раздел **Дополнительные возможности**.

8. Нажмите на кнопку **Настройка** в подразделе **Доверенная зона**.

   Откроется окно **Доверенная зона**.

Настройте доверенную зону в соответствии с вашими требованиями.

Настройка параметров доверенной зоны с помощью Плагина управления

По умолчанию доверенная зона применяется ко всем новым политикам и задачам.

Чтобы настроить параметры доверенной зоны, выполните следующие действия:

1. На закладке **Исключения** укажите объекты, которые Kaspersky Embedded Systems Security пропускает при выполнении задачи.

2. На закладке **Доверенные процессы** укажите процессы, которые Kaspersky Embedded Systems Security пропускает при выполнении задачи.

3. Примените маску not-a-virus.

Добавление исключений

Чтобы добавить исключение в доверенную зону в политике Kaspersky Security Center, выполните следующие действия:

1. Откройте окно **Доверенная зона**.

2. На закладке **Исключения** укажите объекты, которые Kaspersky Embedded Systems Security пропускает при проверке:

   - Чтобы создать рекомендуемые исключения, нажмите на кнопку Добавить рекомендуемые исключения.

   - Чтобы импортировать исключения, нажмите на кнопку **Импорт** и в открывшемся окне выберите файлы, которые Kaspersky Embedded Systems Security будет считать доверенными.

   - Чтобы вручную указать условия, при выполнении которых файл будет считаться доверенным, нажмите на кнопку **Добавить**.

     Откроется окно **Исключение**.

3. В разделе **Не проверять объект при выполнении следующих условий** укажите объекты, которые вы хотите исключить из области защиты / проверки, и объекты, которые требуется исключить из обнаруживаемых объектов:

   - Чтобы исключить объект из области защиты или проверки:

     a. Установите флажок **Проверяемый объект**.

     b. Нажмите на кнопку **Изменить**.

Откроется окно **Выбор объекта**.

c. Выберите объект, который вы хотите исключить из области проверки.

> При указании объектов можно использовать маски имени (с помощью символов `?` и `*`) и переменные среды всех типов. Обработка переменных среды (замена переменных на их значения) выполняется Kaspersky Embedded Systems Security при запуске задачи или при применении новых параметров к запущенной задаче (не применимо к задачам проверки по требованию). Kaspersky Embedded Systems Security обрабатывает переменные среды с правами учетной записи, от имени которой запущена задача. Дополнительная информация о переменных среды приведена в Базе знаний Microsoft.

d. Нажмите на кнопку **OK**.

e. Установите флажок **Учитывать подпапки**, если вы хотите исключить все вложенные файлы и папки указанного объекта из области защиты или проверки.

- Чтобы указать имя обнаруживаемого объекта:

a. Установите флажок **Обнаруживаемые объекты**.

b. Нажмите на кнопку **Изменить**.

Откроется окно **Список обнаруживаемых объектов**.

c. Укажите имя или маску имени обнаруживаемого объекта согласно классификации Вирусной энциклопедии.

d. Нажмите на кнопку **Добавить**.

e. Нажмите на кнопку **OK**.

4. В разделе **Область применения исключения** установите флажки рядом с названиями задач, к которым вы хотите применить исключения.

5. Нажмите на кнопку **OK**.

Исключение отображается в списке на закладке **Исключения** окна **Доверенная зона**.

Добавление доверенных процессов

Чтобы добавить один или несколько процессов в список доверенных, выполните следующие действия:

1. Откройте окно **Доверенная зона**.

2. Выберите закладку **Доверенные процессы**.

3. Установите флажок Не проверять файловые операции резервного копирования, чтобы пропустить проверку операций чтения файлов.

4. Установите флажок **Не проверять файловую активность указанных процессов**, чтобы пропустить проверку файловых операций для доверенных процессов.

5. Нажмите на кнопку **Добавить**.

6. В контекстном меню кнопки выберите один из следующих вариантов:

- **Несколько процессов**

  В открывшемся окне **Добавление доверенных процессов** настройте следующие параметры:

  a. **Использовать полный путь для определения доверенности процессов**

  b. **Использовать хеш файла для определения доверенности процессов**

  c. Чтобы добавить данные на основе исполняемых процессов, нажмите на кнопку **Обзор**.

  d. Выберите исполняемый файл в открывшемся окне.

  > Вы можете добавлять процессы только по одному. Повторите шаги c-d, чтобы добавить другие исполняемые файлы.

  e. Чтобы добавить данные на основе запущенных процессов, нажмите на кнопку **Процессы**.

  f. Выберите процессы в открывшемся окне. Чтобы выбрать несколько процессов, удерживайте клавишу CTRL при выборе.

  g. Нажмите на кнопку **OK**.

  > Учетная запись, с правами которой запускается задача Постоянная защита файлов, должна обладать правами администратора на устройстве с установленной программой Kaspersky Embedded Systems Security, чтобы просматривать список активных процессов. Вы можете отсортировать процессы в списке активных процессов по имени файла, идентификатору процесса (PID) или пути к исполняемому файлу процесса на защищаемом устройстве. Обратите внимание, что вы можете выбрать запущенные процессы, нажав на кнопку **Процессы**, только при работе через Консоль программы на защищаемом устройстве или в параметрах указанного узла в Kaspersky Security Center.

- **Один процесс на основе имени и пути**

  В открывшемся окне **Добавление процесса** выполните следующие действия:

  a. Укажите путь к исполняемому файлу (включая имя файла).

  > При указании объектов можно использовать маски имени (с помощью символов `?` и `*`) и переменные среды всех типов. Обработка переменных среды (замена переменных на их значения) выполняется Kaspersky Embedded Systems Security при запуске задачи или при применении новых параметров к запущенной задаче (не применимо к задачам проверки по требованию). Kaspersky Embedded Systems Security обрабатывает переменные среды с правами учетной записи, от имени которой запущена задача. Дополнительная информация о переменных среды приведена в Базе знаний Microsoft.

  b. Нажмите на кнопку **OK**.

- **Один процесс на основе свойств объекта**

  В открывшемся окне **Добавление доверенного процесса** настройте следующие параметры:

  a. Нажмите на кнопку **Обзор** и выберите процесс.

b. **Использовать полный путь для определения доверенности процесса**

c. **Использовать хеш файла для определения доверенности процесса**

d. Нажмите на кнопку **OK**.

Чтобы добавить выбранный процесс в список доверенных процессов, должен быть выбран как минимум один критерий доверенности.

7. В окне **Доверенная зона** нажмите на кнопку OK.

Выбранный файл или процесс будет добавлен в список доверенных процессов в окне **Доверенная зона**.

Использование маски not-a-virus

Маска not-a-virus позволяет пропускать при проверке файлы легального программного обеспечения и веб-ресурсы, которые могут быть расценены как вредоносные. Маска применяется при работе следующих задач:

- Постоянная защита файлов.
- Проверка по требованию.

Если маска не добавлена в список исключений, Kaspersky Embedded Systems Security выполнит действия, указанные в параметрах задачи, для программ, которые входят в эту категорию.

Чтобы использовать маску not-a-virus, выполните следующие действия:

1. Откройте окно **Доверенная зона**.
2. На закладке **Исключения** в графе **Обнаруживаемые объекты** прокрутите список и выберите строку со значением *not-a-virus:**, если флажок снят.
3. Нажмите на кнопку OK.

Новые параметры будут применены.

Управление доверенной зоной с помощью Консоли программы

В этом разделе описана навигация в интерфейсе Консоли программы и настройка доверенной зоны для защищаемого устройства.

Использование доверенной зоны для задач в Консоли программы

По умолчанию доверенная зона применяется в задаче Постоянная защита файлов, во вновь созданных пользовательских задачах проверки по требованию, а также во всех системных задачах проверки по требованию, кроме задачи Проверка объектов на карантине.

После того как вы включите или выключите доверенную зону, заданные в ней исключения начнут или перестанут действовать в выполняющихся задачах немедленно.

Чтобы включить или выключить применение доверенной зоны в задачах Kaspersky Embedded Systems Security, выполните следующие действия:

1. В дереве Консоли программы откройте контекстное меню задачи, для которой вы хотите настроить использование доверенной зоны.
2. Выберите пункт **Свойства**.

   Откроется окно **Параметры задачи**.
3. В открывшемся окне на закладке **Общие** выполните одно из следующих действий:

   - Чтобы применить доверенную зону в задаче, установите флажок **Применять доверенную зону**.
   - Чтобы выключить применение доверенной зоны в задаче, снимите флажок **Применять доверенную зону**.
4. Чтобы настроить параметры доверенной зоны, перейдите по ссылке в названии флажка **Применять доверенную зону**.

   Откроется окно **Доверенная зона**.

   В окне **Доверенная зона** настройте исключения и доверенные процессы и нажмите на кнопку **OK**.
5. Нажмите на кнопку **OK** в окне **Параметры задачи**, чтобы сохранить изменения.

Настройка параметров доверенной зоны в Консоли программы

Чтобы настроить параметры доверенной зоны, выполните следующие действия:

1. На закладке **Исключения** укажите объекты, которые Kaspersky Embedded Systems Security пропускает при выполнении задачи.
2. На закладке **Доверенные процессы** укажите процессы, которые Kaspersky Embedded Systems Security пропускает при выполнении задачи.
3. Примените доверенную зону для задач программы.
4. Примените маску not-a-virus.

Добавление исключений в доверенную зону

Чтобы вручную добавить исключение в доверенную зону в Консоли программы, выполните следующие действия:

1. В дереве Консоли программы откройте контекстное меню узла **Kaspersky Embedded Systems Security**.
2. Выберите в меню пункт **Настроить параметры доверенной зоны**.

   Откроется окно **Доверенная зона**.
3. Выберите закладку **Исключения**.
4. Нажмите на кнопку **Добавить**.

Откроется окно **Исключение**.

5. В разделе **Не проверять объект при выполнении следующих условий** укажите объекты, которые вы хотите исключить из области защиты / проверки, и объекты, которые требуется исключить из обнаруживаемых объектов:

   - Чтобы исключить объект из области защиты или проверки:

     a. Установите флажок **Проверяемый объект**.

     b. Нажмите на кнопку **Изменить**.

     Откроется окно **Выбор объекта**.

     c. Выберите объект, который вы хотите исключить из области проверки.

     > При указании объектов можно использовать маски имени (с помощью символов `?` и `*`) и переменные среды всех типов. Обработка переменных среды (замена переменных на их значения) выполняется Kaspersky Embedded Systems Security при запуске задачи или при применении новых параметров к запущенной задаче (не применимо к задачам проверки по требованию). Kaspersky Embedded Systems Security обрабатывает переменные среды с правами учетной записи, от имени которой запущена задача. Дополнительная информация о переменных среды приведена в Базе знаний Microsoft.

     d. Нажмите на кнопку **ОК**.

     e. Установите флажок **Учитывать подпапки**, если вы хотите исключить все вложенные файлы и папки указанного объекта из области защиты или проверки.

   - Чтобы указать имя обнаруживаемого объекта:

     a. Установите флажок **Обнаруживаемые объекты**.

     b. Нажмите на кнопку **Изменить**.

     Откроется окно **Список обнаруживаемых объектов**.

     c. Укажите имя или маску имени обнаруживаемого объекта согласно классификации Вирусной энциклопедии.

     d. Нажмите на кнопку **Добавить**.

     e. Нажмите на кнопку **ОК**.

6. В разделе **Область применения исключения** установите флажки рядом с названиями задач, к которым вы хотите применить исключения.

7. Нажмите на кнопку **ОК**.

Исключение отображается в списке на закладке **Исключения** окна **Доверенная зона**.

Добавление доверенных процессов

Вы можете добавить процесс в список доверенных процессов одним из следующих способов:

- выбрать процесс из списка процессов, выполняемых на защищаемом устройстве;
- выбрать исполняемый файл процесса независимо от того, выполняется ли процесс в текущий момент.

Если исполняемый файл процесса изменится, Kaspersky Embedded Systems Security исключит этот процесс из списка доверенных процессов.

Чтобы добавить один или несколько процессов в список доверенных, выполните следующие действия:

1. В дереве Консоли программы откройте контекстное меню узла **Kaspersky Embedded Systems Security**.
2. Выберите в меню пункт **Настроить параметры доверенной зоны**.

   Откроется окно **Доверенная зона**.
3. Выберите закладку **Доверенные процессы**.
4. Установите флажок **Не проверять файловые операции резервного копирования**, чтобы пропустить проверку операций чтения файлов.
5. Установите флажок **Не проверять файловую активность указанных процессов**, чтобы пропустить проверку файловых операций для доверенных процессов.
6. Нажмите на кнопку **Добавить**.
7. В контекстном меню кнопки выберите один из следующих вариантов:

   - **Несколько процессов**

     В открывшемся окне **Добавление доверенных процессов** настройте следующие параметры:

     a. **Использовать полный путь для определения доверенности процессов**

     b. **Использовать хеш файла для определения доверенности процессов**

     c. Чтобы добавить данные на основе исполняемых процессов, нажмите на кнопку **Обзор**.

     d. Выберите исполняемый файл в открывшемся окне.

     Вы можете добавлять процессы только по одному. Повторите шаги c-d, чтобы добавить другие исполняемые файлы.

     e. Чтобы добавить данные на основе запущенных процессов, нажмите на кнопку **Процессы**.

     f. Выберите процессы в открывшемся окне. Чтобы выбрать несколько процессов, удерживайте клавишу **CTRL** при выборе.

     g. Нажмите на кнопку **OK**.

Учетная запись, с правами которой запускается задача Постоянная защита файлов, должна обладать правами администратора на устройстве с установленной программой Kaspersky Embedded Systems Security, чтобы просматривать список активных процессов. Вы можете отсортировать процессы в списке активных процессов по имени файла, идентификатору процесса (PID) или пути к исполняемому файлу процесса на защищаемом устройстве. Обратите внимание, что вы можете выбрать запущенные процессы, нажав на кнопку **Процессы**, только при работе через Консоль программы на защищаемом устройстве или в параметрах указанного узла в Kaspersky Security Center.

- **Один процесс на основе имени и пути**

  В открывшемся окне **Добавление процесса** выполните следующие действия:

  a. Укажите путь к исполняемому файлу (включая имя файла).

  При указании объектов можно использовать маски имени (с помощью символов `?` и `*`) и переменные среды всех типов. Обработка переменных среды (замена переменных на их значения) выполняется Kaspersky Embedded Systems Security при запуске задачи или при применении новых параметров к запущенной задаче (не применимо к задачам проверки по требованию). Kaspersky Embedded Systems Security обрабатывает переменные среды с правами учетной записи, от имени которой запущена задача. Дополнительная информация о переменных среды приведена в Базе знаний Microsoft.

  b. Нажмите на кнопку **OK**.

- **Один процесс на основе свойств объекта**

  В открывшемся окне **Добавление доверенного процесса** настройте следующие параметры:

  a. Нажмите на кнопку **Обзор** и выберите процесс.

  b. **Использовать полный путь для определения доверенности процесса**

  c. **Использовать хеш файла для определения доверенности процесса**

  d. Нажмите на кнопку **OK**.

  Чтобы добавить выбранный процесс в список доверенных процессов, должен быть выбран как минимум один критерий доверенности.

8. В окне **Доверенная зона** нажмите на кнопку **OK**.

Выбранный файл или процесс будет добавлен в список доверенных процессов в окне **Доверенная зона**.

Использование маски not-a-virus

Маска not-a-virus позволяет пропускать при проверке файлы легального программного обеспечения и веб-ресурсы, которые могут быть расценены как вредоносные. Маска применяется при работе следующих задач:

- Постоянная защита файлов.
- Проверка по требованию.

Если маска не добавлена в список исключений, Kaspersky Embedded Systems Security выполнит действия, указанные в параметрах задачи, для программ и веб-ресурсов, которые входят в эту категорию.

Чтобы использовать маску not-a-virus, выполните следующие действия:

1. В дереве Консоли программы откройте контекстное меню узла **Kaspersky Embedded Systems Security**.
2. Выберите в меню пункт **Настроить параметры доверенной зоны**.

   Откроется окно **Доверенная зона**.
3. Выберите закладку **Исключения**.
4. Прокрутите список до элемента *not-a-virus:**.
5. Установите соответствующий флажок, если он снят.
6. Нажмите на кнопку **OK**.

Новые параметры будут применены.

Управление доверенной зоной с помощью Веб-плагина

Чтобы настроить доверенную зону с помощью Веб-плагина, выполните следующие действия:

1. В главном окне веб-консоли выберите **Устройства** → **Политики и профили**.
2. Выберите политику, которую вы хотите настроить.
3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.
4. Выберите раздел **Дополнительные возможности**.
5. Нажмите на кнопку **Параметры** в подразделе **Доверенная зона**.
6. Настройте доверенную зону в соответствии с вашими требованиями.

Защита от эксплойтов

Этот раздел содержит инструкции по настройке параметров защиты памяти процессов от эксплуатации уязвимостей.

О защите от эксплойтов

Kaspersky Embedded Systems Security предоставляет возможность защитить память процессов от эксплойтов. Эта возможность реализована в компоненте Защита от эксплойтов. Вы можете изменять статус активности компонента, а также настраивать параметры защиты процессов от эксплуатации уязвимостей.

Компонент выполняет защиту памяти процессов от эксплойтов с помощью внедрения внешнего Агента защиты процессов (далее "Агент") в защищаемый процесс.

Агент защиты процессов – это динамически загружаемый модуль Kaspersky Embedded Systems Security, который внедряется в защищаемые процессы с целью контроля их целостности и снижения рисков эксплуатации уязвимостей.

Функционирование Агента внутри защищаемого процесса зависит от итераций запуска и остановки этого процесса: первичная загрузка Агента в процесс, добавленный в список защищаемых, возможна только при перезапуске процесса. Выгрузка Агента из процесса после его удаления из списка защищаемых также возможна только после перезапуска процесса.

Выгрузка Агента из защищаемых процессов предполагает необходимость их остановки: при удалении компонента Защита от эксплойтов программа выполняет заморозку среды и форсирует выгрузку Агента из защищаемых процессов. Если при удалении компонента Агент внедрен хотя бы в один из защищаемых процессов, вам нужно завершить данный процесс. Может потребоваться перезагрузка защищаемого устройства (например, при защите системного процесса).

При обнаружении признаков атаки эксплойта на защищаемый процесс Kaspersky Embedded Systems Security выполняет одно из следующих действий:

- завершает процесс при попытке эксплуатации уязвимости;
- сообщает о факте дискредитации уязвимости в процессе.

Вы можете остановить защиту процессов одним из следующих способов:

- удалить компонент;
- удалить процесс из списка защищаемых и перезапустить его.

Служба Kaspersky Security Exploit Prevention

Для максимальной эффективности компоненту Защита от эксплойтов требуется наличие службы Kaspersky Security Exploit Prevention на защищаемом устройстве. Эта служба входит в состав рекомендуемой установки совместно с компонентом Защита от эксплойтов. Во время установки службы на защищаемое устройство создается и запускается процесс kavfswh. Он передает информацию о защищаемых процессах от компонентов Агенту защиты.

После остановки службы Kaspersky Security Exploit Prevention программа продолжает защищать процессы, которые были добавлены в список защищаемых, а также загружается в новые добавленные процессы и применяет все доступные техники защиты от эксплойтов для защиты памяти процессов.

Если на устройстве установлена операционная система Windows 10 или более поздних версий, программа не будет продолжать защищать процессы и память процессов после остановки службы Kaspersky Security Exploit Prevention.

В случае остановки службы Kaspersky Security Exploit Prevention программа не будет получать данные о событиях, происходящих с защищаемыми процессами (в том числе данные об атаках эксплойтов и о завершении процессов). Также Агент не сможет получать данные о новых параметрах защиты и о добавлении новых процессов в список защищаемых процессов.

Режимы защиты от эксплойтов

Вы можете настраивать действия по снижению рисков эксплуатации уязвимостей в защищаемых процессах, выбрав один из следующих режимов:

- **Завершать скомпрометированные процессы**: применяйте данный режим, чтобы завершать процесс при попытке эксплуатации уязвимости.

  При обнаружении попытки эксплуатации уязвимости в защищаемом процессе, которому присвоен уровень "критический" в операционной системе, Kaspersky Embedded Systems Security не выполняет завершение такого процесса независимо от режима, указанного в параметрах компонента Защита от эксплойтов.

- **Только сообщать**: применяйте этот режим, чтобы получать данные о фактах эксплуатации уязвимостей в защищаемых процессах с помощью событий в журнале безопасности.

  В этом режиме Kaspersky Embedded Systems Security регистрирует все попытки эксплуатации уязвимостей посредством создания событий.

Управление защитой от эксплойтов с помощью Плагина управления

В этом разделе описана навигация в интерфейсе Плагина управления и настройка параметров компонента для защищаемых устройств в сети.

Навигация

В этом разделе описан переход к требуемым параметрам задачи с помощью интерфейса.

Переход к параметрам политики для защиты от эксплойтов

Чтобы перейти к параметрам защиты от эксплойтов в политике Kaspersky Security Center, выполните следующие действия:

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой вы хотите настроить задачу.
3. Выберите закладку **Политики**.
4. Откройте окно свойств политики двойным щелчком мыши на имени политики, которую вы хотите настроить.
5. В открывшемся окне **Свойства: <Имя политики>** перейдите в раздел **Постоянная защита компьютера**.
6. Нажмите на кнопку **Настройка** в подразделе **Защита от эксплойтов**.

   Откроется окно **Защита от эксплойтов**.

Настройте защиту от эксплойтов в соответствии с вашими требованиями.

Переход к окну параметров защиты от эксплойтов

Чтобы перейти к окну свойства для защиты от эксплойтов, выполните следующие действия:

1. Разверните узел **Управляемые устройства** в дереве Консоли администрирования Kaspersky Security Center.
2. Выберите группу администрирования, для которой вы хотите настроить задачу.
3. Выберите закладку **Устройства**.
4. Откройте окно **Свойства: <Имя защищаемого устройства>** одним из следующих способов:
   - двойным щелчком мыши на имени защищаемого устройства;
   - выбрав пункт **Свойства** в контекстном меню защищаемого устройства.

   Откроется окно **Свойства: <Имя защищаемого устройства>**.
5. В разделе **Программы** выберите **Kaspersky Embedded Systems Security**.
6. Нажмите на кнопку **Свойства**.

   Откроется окно **Параметры программы Kaspersky Embedded Systems Security**.
7. Перейдите в раздел **Постоянная защита компьютера**.
8. Нажмите на кнопку **Настройка** в подразделе **Защита от эксплойтов**.

   Откроется окно **Защита от эксплойтов**.

Настройте защиту от эксплойтов в соответствии с вашими требованиями.

Настройка защиты памяти процессов

Чтобы настроить параметры защиты от эксплойтов для процессов, добавленных в список защищенных, выполните следующие действия:

1. Откройте окно **Защита от эксплойтов**.
2. В разделе **Защита памяти процессов** настройте следующие параметры:
   - **Защищать процессы от эксплуатации уязвимостей в режиме**
     - **Завершать скомпрометированные процессы**
     - **Только сообщать**
3. В разделе **Действия по защите** настройте следующие параметры:
   - **Сообщать о скомпрометированных процессах посредством службы терминалов**
   - **Защищать процессы от эксплуатации уязвимостей вне зависимости от статуса службы Kaspersky Security**
4. В окне **Защита от эксплойтов** нажмите на кнопку **OK**.

Kaspersky Embedded Systems Security сохранит и применит настроенные параметры защиты памяти процессов.

Добавление процесса в область защиты

Компонент Защита от эксплойтов по умолчанию защищает несколько процессов. Можно исключить процессы из области защиты, сняв соответствующие флажки в списке процессов.

Чтобы добавить процесс в список защищаемых процессов, выполните следующие действия:

1. Откройте окно **Защита от эксплойтов**.
2. На закладке **Защищаемые процессы** нажмите на кнопку **Обзор**.

   Откроется окно проводника Windows.
3. Выберите процесс, который вы хотите добавить в список.
4. Нажмите на кнопку **Открыть**.

   Имя процесса будет отображено в строке.
5. Нажмите на кнопку **Добавить**.

   Указанный процесс добавится в список защищаемых процессов.
6. Выберите добавленный процесс.
7. Нажмите на кнопку **Указать техники защиты от эксплойта**.

   Откроется окно **Техники защиты от эксплойта**.
8. Выберите один из следующих вариантов применения техник снижения рисков:
   - **Применять все доступные техники защиты от эксплойта**

Если выбран этот вариант, редактирование списка недоступно. По умолчанию будут применяться все доступные для процесса техники.

- **Применять указанные техники защиты от эксплойта**

  Если выбран этот вариант, вы можете отредактировать список применяемых техник снижения риска.

  a. Для этого установите флажки напротив техник, которые вы хотите применять для защиты выбранного процесса.

  b. Установите или снимите флажок **Применять технику Attack Surface Reduction**.

9. Настройте параметры работы для техники защиты Attack Surface Reduction (ASR):

   - Внесите названия модулей, запуск которых из защищаемого процесса будет запрещен, в поле **Запрещать модули**.
   - В поле **Не запрещать модули, если запущено в Зоне Интернета** установите флажки напротив тех вариантов, для которых вы хотите разрешить запуск модулей:
     - **Интернет**
     - **Интранет**
     - **Доверенные сайты**
     - **Сайты с ограниченным доступом**
     - **Компьютер**

   Данные параметры применимы только для Internet Explorer®.

10. Нажмите на кнопку **OK**.

    Процесс будет добавлен в область защиты задачи.

Управление защитой от эксплойтов с помощью Консоли программы

В этом разделе описана навигация в интерфейсе Консоли программы и настройка параметров компонента на защищаемом устройстве.

Навигация

В этом разделе описан переход к требуемым параметрам задачи с помощью интерфейса.

Переход к основным параметрам защиты от эксплойтов

*Чтобы перейти к окну **Параметры защиты от эксплуатации уязвимостей**, выполните следующие действия:*

1. В дереве Консоли программы выберите узел **Kaspersky Embedded Systems Security**.
2. В контекстном меню выберите пункт **Защита от эксплойтов: общие параметры защиты**.

   Откроется окно **Параметры защиты от эксплуатации уязвимостей**.

Настройте общие параметры защиты от эксплойтов в соответствии с вашими требованиями.

Переход к параметрам защиты процессов при защите от эксплойтов

*Чтобы перейти к окну **Параметры защиты процессов**, выполните следующие действия:*

1. В дереве Консоли программы выберите узел **Kaspersky Embedded Systems Security**.
2. В контекстном меню выберите пункт **Защита от эксплойтов: параметры защиты процессов**.

   Откроется окно **Параметры защиты процессов**.

Настройте параметры защиты процессов для защиты от эксплойтов в соответствии с вашими требованиями.

Настройка защиты памяти процессов

Чтобы добавить процесс в список защищаемых процессов, выполните следующие действия:

1. Откройте окно **Параметры защиты от эксплуатации уязвимостей**.
2. В разделе **Защита памяти процессов** настройте следующие параметры:
   - **Защищать процессы от эксплуатации уязвимостей в режиме**
     - **Завершать скомпрометированные процессы**
     - **Только сообщать**
3. В разделе **Действия по защите** настройте следующие параметры:
   - **Сообщать о скомпрометированных процессах посредством службы терминалов**
   - **Защищать процессы от эксплуатации уязвимостей вне зависимости от статуса службы Kaspersky Security**
4. В окне **Параметры защиты от эксплуатации уязвимостей** нажмите на кнопку **OK**.

Kaspersky Embedded Systems Security сохранит и применит настроенные параметры защиты памяти процессов.

Добавление процесса в область защиты

Компонент Защита от эксплойтов по умолчанию защищает несколько процессов. Вы можете исключить какой-либо процесс из защиты, сняв флажок в соответствующей строке процесса.

Чтобы добавить процесс в список защищаемых процессов, выполните следующие действия:

1. Откройте окно **Параметры защиты процессов**.

2. Чтобы защитить процесс от компрометации и снизить возможное влияние эксплуатации уязвимостей, выполните следующие действия:

   a. Нажмите на кнопку **Обзор**.

      Откроется стандартное окно Microsoft Windows **Открыть**.

   b. В открывшемся окне выберите процесс, который вы хотите добавить в список.

   c. Нажмите на кнопку **Открыть**.

   d. Нажмите на кнопку **Добавить**.

      Указанный процесс добавится в список защищаемых процессов.

3. Выберите добавленный процесс в списке.

4. Текущая конфигурация отображается на закладке **Параметры защиты процесса**:

   - **Имя процесса**
   - **Выполняется сейчас**
   - **Применяемые техники защиты**
   - **Снижение области действия процесса (параметры техники Attack Surface Reduction)**

5. Чтобы изменить применяемые к процессу техники защиты от эксплойтов, выберите закладку **Техники защиты**.

6. Выберите один из следующих вариантов применения техник снижения рисков:

   - **Применять все доступные техники защиты от эксплойта**

     Если выбран этот вариант, редактирование списка недоступно. По умолчанию будут применяться все доступные для процесса техники.

   - **Применять указанные техники защиты от эксплойта**

     Если выбран этот вариант, вы можете отредактировать список применяемых техник снижения риска.

     a. Для этого установите флажки напротив техник, которые вы хотите применять для защиты выбранного процесса.

7. Настройте параметры работы для техники защиты Attack Surface Reduction (ASR):

   - Внесите названия модулей, запуск которых из защищаемого процесса будет запрещен, в поле **Запрещать загрузку модулей**.
   - В разделе **Не запрещать модули, если они запущены в зоне интернета** установите флажки напротив тех вариантов, для которых вы хотите разрешить запуск модулей:
     - **Интернет**
     - **Интранет**
     - **Доверенные сайты**

- **Сайты с ограниченным доступом**
- **Компьютер**

> Данные параметры применимы только для Internet Explorer®.

8. Нажмите на кнопку **Сохранить**.

Процесс будет добавлен в область защиты задачи.

Управление защитой от эксплойтов с помощью Веб-плагина

В этом разделе описана навигация в интерфейсе Веб-плагина и настройка параметров компонента на защищаемом устройстве.

Настройка защиты памяти процессов

Чтобы настроить параметры защиты от эксплойтов для процессов, добавленных в список защищенных, выполните следующие действия:

1. В главном окне веб-консоли выберите **Устройства** → **Политики и профили**.
2. Выберите политику, которую вы хотите настроить.
3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.
4. Перейдите в раздел **Постоянная защита компьютера**.
5. Нажмите на кнопку **Параметры** в подразделе **Защита от эксплойтов**.
6. Откройте закладку **Параметры защиты от эксплойтов**.
7. В разделе **Защита памяти процессов** настройте следующие параметры:
   - Защищать процессы от эксплуатации уязвимостей в режиме
     - Завершать скомпрометированные процессы
     - Только сообщать о компрометации процесса
8. В разделе **Действия по защите** настройте следующие параметры:
   - Сообщать о скомпрометированных процессах посредством службы терминалов
   - Защищать процессы от эксплуатации уязвимостей вне зависимости от статуса службы Kaspersky Security
9. В окне **Защита от эксплойтов** нажмите на кнопку **OK**.

Kaspersky Embedded Systems Security сохранит и применит настроенные параметры защиты памяти процессов.

Добавление процесса в область защиты

Чтобы настроить параметры защиты от эксплойтов для процессов, добавленных в список защищенных, выполните следующие действия:

1. В главном окне веб-консоли выберите **Устройства** → **Политики и профили**.
2. Выберите политику, которую вы хотите настроить.
3. В открывшемся окне **<Имя политики>** выберите закладку **Параметры программы**.
4. Перейдите в раздел **Постоянная защита компьютера**.
5. Нажмите на кнопку **Параметры** в подразделе **Защита от эксплойтов**.
6. Перейдите на закладку **Защищаемые процессы**.
7. Нажмите на кнопку **Добавить**.
8. Откроется окно **Техники защиты от эксплойта**.
9. Укажите название процесса.
10. Выберите один из следующих вариантов применения техник снижения рисков:

    - **Применять все доступные техники защиты от эксплойта**

      Если выбран этот вариант, редактирование списка недоступно. По умолчанию будут применяться все доступные для процесса техники.

    - **Применять указанные техники защиты от эксплойта**

      Если выбран этот вариант, вы можете отредактировать список применяемых техник снижения риска.

      a. Для этого установите флажки напротив техник, которые вы хотите применять для защиты выбранного процесса.

      b. Установите или снимите флажок **Применять технику Attack Surface Reduction**.

11. Настройте параметры работы для техники защиты Attack Surface Reduction (ASR):

    - Внесите названия модулей, запуск которых из защищаемого процесса будет запрещен, в поле **Запрещать модули**.
    - В поле **Не запрещать модули, если запущено в Зоне Интернета** установите флажки напротив тех вариантов, для которых вы хотите разрешить запуск модулей:
        - **Интернет**
        - **Интранет**
        - **Доверенные сайты**

- **Сайты с ограниченным доступом**
- **Компьютер**

Данные параметры применимы только для Internet Explorer®.

12. Нажмите на кнопку **OK**.

Процесс будет добавлен в область защиты задачи.

Техники защиты от эксплойтов

Техники защиты от эксплойтов

Техника защиты от эксплойтов	Описание
Data Execution Prevention (DEP)	Предотвращение выполнения данных - запрет исполнения произвольного кода в защищенной области памяти.
Address Space Layout Randomization (ASLR)	Изменение расположения структур данных в адресном пространстве процесса.
Structured Exception Handler Overwrite Protection (SEHOP)	Подмена записи в структуре исключений или подмена обработчика исключений.
Null Page Allocation	Предотвращение переориентации нулевого указателя.
LoadLibrary Network Call Check (Anti ROP)	Защита от загрузки динамических библиотек с сетевых путей.
Executable Stack (Anti ROP)	Запрет на несанкционированное исполнение областей стека.
Anti RET Check (Anti ROP)	Проверка безопасного вызова функции через CALL инструкцию.
Anti Stack Pivoting (Anti ROP)	Защита от перемещения указателя стека ESP на эксплуатируемый адрес.
Simple Export Address Table Access Monitor (EAT Access Monitor & EAT Access Monitor via Debug Register)	Защита доступа на чтение таблицы экспорта адресов (Export Address Table) для модулей kernel32.dll, kernelbase.dll, ntdll.dll.
Heap Spray Allocation (Heapspray)	Защита от выделения памяти под исполнение вредоносного кода.
Execution Flow Simulation (Anti Return Oriented Programming)	Обнаружение потенциально опасных цепочек инструкций (возможный ROP гаджет) в компоненте Windows API.
IntervalProfile Calling Monitor (Ancillary Function Driver Protection (AFDP))	Защита от эскалации привилегий через уязвимость в драйвере AFD (выполнение произвольного кода на нулевом кольце через вызов QueryIntervalProfile).
Attack Surface Reduction (ASR)	Блокирование запуска уязвимых модулей через защищаемый процесс.
Anti Process Hollowing (Hollowing)	Защита от создания и запуска вредоносных копий доверенных процессов.
Anti AtomBombing (APC)	Защита от эксплуатации глобальных атомных таблиц через асинхронные вызовы процедур (APC).
Anti CreateLocalThread (RThreadRemote)	Сторонний процесс создал поток в защищаемом процессе.

Anti CreateRemoteThread (RThreadRemote)	Защита внедрения потока защищаемого процесса в другой процесс.

Интеграция со сторонними системами

Этот раздел содержит описание интеграции Kaspersky Embedded Systems Security с функциями и технологиями сторонних производителей.

Счетчики производительности для программы Системный монитор

Этот раздел содержит информацию о счетчиках производительности для программы Системный монитор Microsoft Windows, которые регистрирует Kaspersky Embedded Systems Security во время установки.

О счетчиках производительности Kaspersky Embedded Systems Security

В состав устанавливаемых компонентов Kaspersky Embedded Systems Security по умолчанию включен компонент Счетчики производительности. Во время установки Kaspersky Embedded Systems Security регистрирует свои счетчики производительности для программы Системный монитор Microsoft Windows.

С помощью счетчиков Kaspersky Embedded Systems Security вы можете контролировать производительность программы во время выполнения задач постоянной защиты компьютера. Вы можете обнаружить узкие места и недостаточность ресурсов при совместной работе с другими программами. Вы можете диагностировать сбои в работе и неоптимальную настройку Kaspersky Embedded Systems Security.

Вы можете просматривать счетчики производительности Kaspersky Embedded Systems Security, открыв консоль **Производительность** Панели управления Windows в разделе **Администрирование**.

В следующих разделах приведены определения счетчиков, рекомендованные интервалы считывания показаний, пороговые значения и рекомендованные значения параметров Kaspersky Embedded Systems Security для случаев, когда значения счетчиков превышают пороговые значения.

Общее количество отвергнутых запросов

Общее количество отвергнутых запросов

Название	Общее количество отвергнутых запросов
Определение	Общее количество запросов драйвера файловых перехватов на обработку объектов, которые не были приняты процессами программы; рассчитывается с момента последнего запуска Kaspersky Embedded Systems Security. Программа пропускает объекты, запросы на обработку которых отвергаются процессами Kaspersky Embedded Systems Security.
Назначение	Счетчик позволяет обнаруживать следующие ситуации: • снижение эффективности постоянной защиты компьютера из-за повышенной нагрузки на процессы Kaspersky Embedded Systems Security; • прерывание постоянной защиты компьютера из-за отказа диспетчера файловых перехватов.
Нормальное / пороговое значение	0 / 1

Рекомендуемый интервал считывания показаний	1 час
Рекомендации по настройке, если значение превышает пороговое	Количество отвергнутых запросов на обработку соответствует количеству пропущенных объектов. Возможны следующие ситуации в зависимости от поведения счетчика: • Счетчик показывает несколько запросов, отвергнутых в течение длительного времени: все процессы Kaspersky Embedded Systems Security были полностью загружены, поэтому программа Kaspersky Embedded Systems Security не смогла проверить объекты. Чтобы исключить пропуск объектов, увеличьте количество процессов программы для задач постоянной защиты компьютера. Можно использовать такие параметры Kaspersky Embedded Systems Security, как **Максимальное количество активных процессов** и **Количество процессов для постоянной защиты**. • Количество отвергнутых запросов значительно превышает критический порог и быстро растет: отказал диспетчер файловых перехватов. Kaspersky Embedded Systems Security не проверяет объекты при обращении к ним. Перезапустите Kaspersky Embedded Systems Security.

Общее количество пропущенных запросов

Общее количество пропущенных запросов

Название	Общее количество пропущенных запросов
Определение	Общее количество запросов драйвера файловых перехватов на обработку объектов, принятых Kaspersky Embedded Systems Security, но не отправивших события о завершении обработки; рассчитывается с момента последнего запуска программы. Если запрос на обработку объекта, принятый одним из рабочих процессов, не отправил события о завершении обработки, драйвер передает этот запрос другому процессу и значение счетчика **Общее количество пропущенных запросов** увеличивается на 1. Если драйвер перебрал все рабочие процессы и ни один из них не принял запрос на обработку (был занят) или не отправил события о завершении обработки, Kaspersky Embedded Systems Security пропускает такой объект и значение счетчика **Общее количество пропущенных запросов** увеличивается на 1.
Назначение	Счетчик позволяет обнаруживать снижение производительности из-за сбоев диспетчера файловых перехватов.
Нормальное / пороговое значение	0 / 1
Рекомендуемый интервал считывания показаний	1 час
Рекомендации по настройке, если значение превышает пороговое	Если значение счетчика отличается от нуля, это означает, что зависли и простаивают один или несколько потоков диспетчера файловых перехватов. Значение счетчика соответствует количеству потоков, простаивающих в текущий момент. Если скорость проверки не удовлетворительна, перезапустите Kaspersky Embedded Systems Security, чтобы восстановить простаивающие потоки.

Количество запросов, не обработанных из-за нехватки системных ресурсов

Количество запросов, не обработанных из-за нехватки системных ресурсов

Название	Количество запросов, не обработанных из-за нехватки системных ресурсов (Number of requests not processed due to lack of resources)
Определение	Общее количество запросов драйвера файловых перехватов, не обработанных из-за нехватки системных ресурсов (например, оперативной памяти); рассчитывается с момента последнего запуска Kaspersky Embedded Systems Security. Kaspersky Embedded Systems Security пропускает запросы на обработку объектов, которые не обрабатываются драйвером файловых перехватов.
Назначение	Счетчик позволяет обнаруживать и устранять возможное снижение качества постоянной защиты компьютера, возникающее из-за недостаточности системных ресурсов.
Нормальное / пороговое значение	0 / 1
Рекомендуемый интервал считывания показаний	1 час
Рекомендации по настройке, если значение превышает пороговое	Если значение счетчика отличается от нуля, рабочим процессам Kaspersky Embedded Systems Security требуется больший объем оперативной памяти для обработки запросов. Возможно, активные процессы других программ используют всю доступную оперативную память.

Количество запросов, отправленных на обработку

Количество запросов, отправленных на обработку

Название	Количество запросов, отправленных на обработку.
Определение	Количество объектов, ожидающих обработки рабочими процессами.
Назначение	Счетчик позволяет отслеживать загрузку рабочих процессов Kaspersky Embedded Systems Security и общий уровень файловой активности на защищаемом устройстве.
Нормальное / пороговое значение	Значение счетчика может изменяться в зависимости от уровня файловой активности на защищаемом устройстве.
Рекомендуемый интервал считывания показаний	1 мин.
Рекомендации по настройке, если значение превышает пороговое	Недоступно

Среднее количество потоков диспетчера файловых перехватов

Среднее количество потоков диспетчера файловых перехватов

Название	Среднее количество потоков диспетчера файловых перехватов (Average number of file interception dispatcher streams)
Определение	Количество потоков диспетчера файловых перехватов в одном процессе и среднее по всем процессам, участвующим в задачах постоянной защиты компьютера.
Назначение	Счетчик позволяет обнаруживать и устранять возможное снижение уровня постоянной защиты компьютера из-за полной загрузки процессов Kaspersky Embedded Systems Security.
Нормальное / пороговое значение	Варьируется / 40.
Рекомендуемый интервал считывания показаний	1 мин.
Рекомендации по настройке, если значение превышает пороговое	В каждом рабочем процессе может быть создано до 60 потоков диспетчера файловых перехватов. Если значение счетчика приближается к 60, возникает риск того, что ни одному из рабочих процессов не удастся принять на обработку очередной запрос от драйвера файловых перехватов и Kaspersky Embedded Systems Security пропустит объект. Увеличьте количество процессов Kaspersky Embedded Systems Security для задач постоянной защиты компьютера. Можно использовать такие параметры Kaspersky Embedded Systems Security, как **Максимальное количество активных процессов** и **Количество процессов для постоянной защиты**.

Максимальное количество потоков диспетчера файловых перехватов

Максимальное количество потоков диспетчера файловых перехватов

Название	Максимальное количество потоков диспетчера файловых перехватов (Maximum number of file interception dispatcher streams).
Определение	Количество потоков диспетчера файловых перехватов в одном процессе и максимальное по всем процессам, участвующим в задачах постоянной защиты компьютера.
Назначение	Счетчик позволяет обнаруживать и устранять снижение производительности из-за неравномерного распределения нагрузки в выполняющихся рабочих процессах.
Нормальное / пороговое значение	Варьируется / 40.
Рекомендуемый интервал считывания показаний	1 мин.
Рекомендации по настройке, если значение превышает пороговое	Если значение этого счетчика значительно и продолжительно превышает значение счетчика **Среднее количество потоков диспетчера файловых перехватов**, Kaspersky Embedded Systems Security неравномерно распределяет нагрузку на выполняющиеся процессы. Перезапустите Kaspersky Embedded Systems Security.

Количество элементов в очереди зараженных объектов

Количество элементов в очереди зараженных объектов

Название	Количество элементов в очереди зараженных объектов.
Определение	Количество зараженных объектов, ожидающих обработки (лечения или удаления) в текущий момент.
Назначение	Счетчик позволяет обнаруживать следующие ситуации: • прерывание постоянной защиты компьютера из-за возможного отказа диспетчера файловых перехватов; • перегруженность процессов из-за неравномерного распределения процессорного времени между рабочими процессами и Kaspersky Embedded Systems Security; • вирусную эпидемию.
Нормальное / пороговое значение	Значение счетчика может быть отличным от нуля, пока Kaspersky Embedded Systems Security обрабатывает обнаруженные зараженные или возможно зараженные объекты, но оно возвращается к нулю вскоре после окончания обработки / Значение счетчика остается ненулевым длительное время.
Рекомендуемый интервал считывания показаний	1 мин.
Рекомендации по настройке, если значение превышает пороговое	Если значение счетчика остается ненулевым длительное время: • Kaspersky Embedded Systems Security не обрабатывает объекты (возможно, отказал диспетчер файловых перехватов). Перезапустите Kaspersky Embedded Systems Security. • Не хватает процессорного времени для обработки объектов. Обеспечьте выделение Kaspersky Embedded Systems Security дополнительного процессорного времени, например, снизив нагрузку на защищаемое устройство со стороны других программ. • Возникла вирусная эпидемия. О возникновении вирусной эпидемии свидетельствует большое количество обнаруженных зараженных или возможно зараженных объектов в задаче Постоянная защита файлов. Вы можете просмотреть информацию о количестве обнаруженных объектов в статистике задачи или журнале выполнения задачи.

Количество объектов, обрабатываемых за секунду

Количество объектов, обрабатываемых за секунду

Название	Количество объектов, обрабатываемых за секунду (Number of objects processed per second)
Определение	Количество обработанных объектов, разделенное на количество времени, в течение которого эти объекты были обработаны; рассчитывается за равные промежутки

	времени.
Назначение	Счетчик отражает скорость обработки объектов; позволяет обнаружить и устранить снижение производительности защищаемого устройства, возникшее из-за недостаточности процессорного времени, выделяемого рабочим процессам Kaspersky Embedded Systems Security, или сбоев в работе Kaspersky Embedded Systems Security.
Нормальное / пороговое значение	Варьируется / Нет.
Рекомендуемый интервал считывания показаний	1 мин.
Рекомендации по настройке, если значение превышает пороговое	Значения счетчика зависят от установленных значений параметров Kaspersky Embedded Systems Security и загрузки защищаемого устройства процессами других программ. Отслеживайте среднее значение показаний счетчика в течение продолжительного времени. Если среднее значение показаний счетчика снизилось, то могла возникнуть одна из следующих ситуаций: • Рабочим процессам Kaspersky Embedded Systems Security не хватает процессорного времени для обработки объектов. Обеспечьте выделение Kaspersky Embedded Systems Security дополнительного процессорного времени, например, снизив нагрузку на защищаемое устройство со стороны других программ. • Возник сбой в работе Kaspersky Embedded Systems Security (простаивает несколько потоков). Перезапустите Kaspersky Embedded Systems Security.

Счетчики и ловушки SNMP Kaspersky Embedded Systems Security

Этот раздел содержит информацию о счетчиках и ловушках Kaspersky Embedded Systems Security.

О счетчиках и ловушках SNMP Kaspersky Embedded Systems Security

Если вы включили компонент Счетчики и ловушки SNMP в состав устанавливаемых антивирусных компонентов, вы можете просматривать счетчики и ловушки Kaspersky Embedded Systems Security по протоколу Simple Network Management Protocol (SNMP).

Чтобы просматривать счетчики и ловушки Kaspersky Embedded Systems Security на рабочем месте администратора, запустите на защищаемом устройстве Службу SNMP (SNMP Service), а на рабочем месте администратора – Службу SNMP (SNMP Service) и Службу ловушек SNMP (SNMP Trap Service).

SNMP-счетчики Kaspersky Embedded Systems Security

Этот раздел содержит таблицы с описанием параметров SNMP-счетчиков Kaspersky Embedded Systems Security.

Счетчики производительности

Счетчики производительности

Счетчик	Определение
currentRequestsAmount	Количество запросов, отправленных на обработку
currentInfectedQueueLength	Количество элементов в очереди зараженных объектов
currentObjectProcessingRate	Количество объектов, обрабатываемых за секунду
currentWorkProcessesNumber	Количество рабочих процессов Kaspersky Embedded Systems Security в текущий момент

Счетчики карантина

Счетчики карантина

Счетчик	Определение
totalObjects	Количество объектов в папке карантина в текущий момент
totalSuspiciousObjects	Количество возможно зараженных объектов в папке карантина в текущий момент
currentStorageSize	Общий объем данных в папке карантина (МБ)

Счетчик резервного хранилища

Счетчик резервного хранилища

Счетчик	Определение
currentBackupStorageSize	Общий объем данных в папке резервного хранилища (МБ)

Общие счетчики

Общие счетчики

Счетчик	Определение
lastCriticalAreasScanAge	Период с момента проведения последней полной проверки важных областей защищаемого устройства (промежуток времени в секундах с момента завершения задачи Проверка важных областей).
licenseExpirationDate	Дата окончания срока действия лицензии. Если добавлен активный и дополнительный ключ, отображается дата окончания срока действия лицензии, связанной с дополнительным ключом.
currentApplicationUptime	Время работы Kaspersky Embedded Systems Security с момента его последнего запуска, в сотых долях секунды.

Счетчик обновлений

Счетчик обновлений

Счетчик	Определение
avBasesAge	"Возраст" баз (промежуток времени в сотых долях секунды с момента создания последних установленных обновлений баз)

Счетчики постоянной защиты файлов

Счетчики постоянной защиты файлов

Счетчик	Определение
totalObjectsProcessed	Общее количество проверенных объектов с момента последнего запуска задачи Постоянная защита файлов
totalInfectedObjectsFound	Общее количество обнаруженных зараженных и других объектов с момента последнего запуска задачи Постоянная защита файлов
totalSuspiciousObjectsFound	Общее количество обнаруженных возможно зараженных объектов с момента последнего запуска задачи Постоянная защита файлов
totalVirusesFound	Общее количество обнаруженных объектов с момента последнего запуска задачи Постоянная защита файлов
totalObjectsQuarantined	Общее количество зараженных, возможно зараженных и прочих объектов, которые программа Kaspersky Embedded Systems Security поместила на карантин; рассчитывается с момента последнего запуска задачи Постоянная защита файлов
totalObjectsNotQuarantined	Общее количество зараженных или возможно зараженных объектов, которые программе Kaspersky Embedded Systems Security не удалось поместить на карантин; рассчитывается с момента последнего запуска задачи Постоянная защита файлов
totalObjectsDisinfected	Общее количество зараженных объектов, которые вылечила программа Kaspersky Embedded Systems Security; рассчитывается с момента последнего запуска задачи Постоянная защита файлов
totalObjectsNotDisinfected	Общее количество зараженных и прочих объектов, которые программе Kaspersky Embedded Systems Security не удалось вылечить; рассчитывается с момента последнего запуска задачи Постоянная защита файлов
totalObjectsDeleted	Общее количество зараженных, возможно зараженных и прочих объектов, которые удалила программа Kaspersky Embedded Systems Security; рассчитывается с момента последнего запуска задачи Постоянная защита файлов
totalObjectsNotDeleted	Общее количество зараженных, возможно зараженных и прочих объектов, которые программе Kaspersky Embedded Systems Security не удалось удалить; рассчитывается с момента последнего запуска задачи Постоянная защита файлов
totalObjectsBackedUp	Общее количество зараженных и прочих объектов, которые программа Kaspersky Embedded Systems Security поместила в резервное хранилище; рассчитывается с момента последнего запуска задачи Постоянная защита файлов

totalObjectsNotBackedUp	Общее количество зараженных и прочих объектов, которые программе Kaspersky Embedded Systems Security не удалось поместить в резервное хранилище; рассчитывается с момента последнего запуска задачи Постоянная защита файлов

SNMP-ловушки Kaspersky Embedded Systems Security и их параметры

В Kaspersky Embedded Systems Security предусмотрены следующие параметры SNMP-ловушек:

- eventThreatDetected: Обнаружен объект.

  В ловушке используются следующие параметры:

  - eventDateAndTime
  - eventSeverity
  - computerName
  - userName
  - objectName
  - threatName
  - detectType
  - detectCertainty

- eventBackupStorageSizeExceeds: Превышен максимальный размер резервного хранилища. Общий объем данных в резервном хранилище превысил значение, заданное параметром **Максимальный размер резервного хранилища (МБ)**. Kaspersky Embedded Systems Security продолжает резервировать зараженные объекты.

  В ловушке используются следующие параметры:

  - eventDateAndTime
  - eventSeverity
  - eventSource

- eventThresholdBackupStorageSizeExceeds: Достигнут порог свободного места в резервном хранилище. Объем свободного места в резервном хранилище меньше или равен значения, заданного параметром **Порог доступного пространства (МБ)**. Kaspersky Embedded Systems Security продолжает резервировать зараженные объекты.

  В ловушке используются следующие параметры:

  - eventDateAndTime
  - eventSeverity
  - eventSource

- eventQuarantineStorageSizeExceeds: Превышен максимальный размер карантина. Общий объем данных в папке карантина превысил значение, заданное параметром **Максимальный размер карантина (МБ)**. Kaspersky Embedded Systems Security продолжает помещать возможно зараженные объекты на карантин.

  В ловушке используются следующие параметры:

  - eventDateAndTime
  - eventSeverity
  - eventSource

- eventThresholdQuarantineStorageSizeExceeds: Достигнут порог свободного места в карантине. Объем свободного места в папке карантина меньше или равен значения, заданного параметром **Порог доступного пространства (МБ)**. Kaspersky Embedded Systems Security продолжает резервировать зараженные объекты.

  В ловушке используются следующие параметры:

  - eventDateAndTime
  - eventSeverity
  - eventSource

- eventObjectNotQuarantined: Ошибка карантина.

  В ловушке используются следующие параметры:

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - userName
  - computerName
  - objectName
  - storageObjectNotAddedEventReason

- eventObjectNotBackuped: Ошибка сохранения копии объекта в резервное хранилище.

  В ловушке используются следующие параметры:

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - objectName
  - userName
  - computerName

- storageObjectNotAddedEventReason

- eventQuarantineInternalError: Внутренняя ошибка карантина.

  В ловушке используются следующие параметры:

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - eventReason

- eventBackupInternalError: Ошибка резервного хранилища.

  В ловушке используются следующие параметры:

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - eventReason

- eventAVBasesOutdated: Базы программы устарели. Количество дней с момента последнего выполнения задачи Обновление баз программы (локальной, групповой или задачи для наборов защищаемых устройств).

  В ловушке используются следующие параметры:

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - days

- eventAVBasesTotallyOutdated: Базы программы сильно устарели. Количество дней с момента последнего выполнения задачи Обновление баз программы (локальной, групповой или задачи для наборов защищаемых устройств).

  В ловушке используются следующие параметры:

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - days

- eventApplicationStarted: программа Kaspersky Embedded Systems Security запущена.

  В ловушке используются следующие параметры:

  - eventSeverity

- eventDateAndTime
- eventSource

- eventApplicationShutdown: программа Kaspersky Embedded Systems Security остановлена.

  В ловушке используются следующие параметры:

  - eventSeverity
  - eventDateAndTime
  - eventSource

- eventCriticalAreasScanWasntPerformForALongTime: Проверка важных областей давно не выполнялась. Количество дней с момента последнего завершения
  задачи Проверка важных областей.

  В ловушке используются следующие параметры:

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - days

- eventLicenseHasExpired: Срок действия лицензии истек.

  В ловушке используются следующие параметры:

  - eventSeverity
  - eventDateAndTime
  - eventSource

- eventLicenseExpiresSoon: Срок действия лицензии скоро истечет. Рассчитывается количество дней, оставшихся до окончания срока действия лицензии.

  В ловушке используются следующие параметры:

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - days

- eventTaskInternalError: Ошибка выполнения задачи.

  В ловушке используются следующие параметры:

  - eventSeverity
  - eventDateAndTime

- eventSource
- errorCode
- knowledgeBaseId
- taskName

- eventUpdateError: Ошибка при выполнении задачи обновления.

  В ловушке используются следующие параметры:

  - eventSeverity
  - eventDateAndTime
  - taskName
  - updaterErrorEventReason

Описания и возможные значения параметров SNMP-ловушек Kaspersky Embedded Systems Security

Ниже приведено описание и допустимые значения параметров ловушек:

- eventDateAndTime: дата и время события.
- eventSeverity: уровень важности.

  Параметр может принимать следующие значения:

  - critical (1) – критический;
  - warning (2) – предупреждение;
  - info (3) – информационный.
- userName: имя пользователя (например, имя пользователя, который пытался получить доступ к зараженному файлу).
- computerName: имя защищаемого устройства (например, имя защищаемого устройства, с которого пользователь пытался получить доступ к зараженному файлу).
- eventSource: функциональный компонент, в работе которого возникло событие.

  Параметр может принимать следующие значения:

  - unknown (0) – функциональный компонент не определен;
  - quarantine (1) – Карантин;
  - backup (2) – Резервное хранилище;
  - reporting (3) – Журналы выполнения задач;

- updates (4)– Обновление;
- realTimeProtection (5) – Постоянная защита файлов;
- onDemandScanning (6) – Проверка по требованию;
- product (7) – событие связано не с работой отдельных компонентов, а с работой Kaspersky Embedded Systems Security в целом;
- systemAudit (8) – Журнал системного аудита.

- eventReason: причина возникновения события.

  Параметр может принимать следующие значения:

  - reasonUnknown (0) – причина не определена.
  - reasonInvalidSettings (1) – только для событий резервного хранилища и карантина. Отображается, если недоступна папка карантина или папка резервного хранилища (недостаточно прав доступа или папка неверно указана в параметрах карантина, например, указан сетевой путь). В этом случае Kaspersky Embedded Systems Security будет использовать папку резервного хранилища или папку карантина, установленную по умолчанию.

- objectName: имя объекта (например, имя файла, в котором обнаружен вирус).
- threatName: имя объекта согласно классификации Вирусной энциклопедии. Это имя входит в полное название объекта, которое Kaspersky Embedded Systems Security возвращает при обнаружении объекта. Вы можете просмотреть полное название обнаруженного объекта в журнале выполнения задачи.
- detectType: тип обнаруженного объекта.

  Параметр может принимать следующие значения:

  - undefined (0) – не определен;
  - virware – классические вирусы и сетевые черви;
  - trojware – троянские программы;
  - malware – прочие вредоносные программы;
  - adware – рекламные программы;
  - pornware – порнографические программы;
  - riskware – легальные программы, которые могут быть использованы злоумышленником для нанесения вреда устройству или личным данным.

- detectCertainty: степень уверенности обнаружения угрозы.

  Параметр может принимать следующие значения:

  - Suspicion (возможно зараженный) – программа Kaspersky Embedded Systems Security обнаружила частичное совпадение участка кода объекта с известным участком вредоносного кода.
  - Sure (зараженный) – программа Kaspersky Embedded Systems Security обнаружила полное совпадение участка кода объекта с известным участком вредоносного кода.

- days: количество дней (например, количество дней до окончания срока действия лицензии).

- errorCode: код ошибки.
- knowledgeBaseId: адрес статьи в базе знаний (например, адрес статьи, описывающей какую-либо ошибку).
- taskName: название задачи.
- updaterErrorEventReason: причина ошибки обновления.

  Параметр может принимать следующие значения:

  - reasonUnknown (0) – причина не определена;
  - reasonAccessDenied – доступ запрещен;
  - reasonUrlsExhausted – список источников обновлений исчерпан;
  - reasonInvalidConfig – неправильный файл конфигурации;
  - reasonInvalidSignature – неверная подпись;
  - reasonCantCreateFolder – невозможно создать папку;
  - reasonFileOperError – файловая ошибка;
  - reasonDataCorrupted – объект поврежден;
  - reasonConnectionReset – сброс соединения;
  - reasonTimeOut – истекло время ожидания при соединении;
  - reasonProxyAuthError – ошибка проверки подлинности на прокси-сервере;
  - reasonServerAuthError – ошибка проверки подлинности на сервере;
  - reasonHostNotFound – устройство не найдено;
  - reasonServerBusy – сервер недоступен;
  - reasonConnectionError – ошибка соединения;
  - reasonModuleNotFound – объект не найден;
  - reasonBlstCheckFailed(16) – ошибка проверки черного списка ключей. Возможно, в момент обновления публиковались обновления баз; повторите обновление через несколько минут.
- storageObjectNotAddedEventReason: причина, по которой объект не был помещен в резервное хранилище или на карантин.

  Параметр может принимать следующие значения:

  - reasonUnknown (0) – причина не определена.
  - reasonStorageInternalError – ошибка базы данных; необходимо восстановление Kaspersky Embedded Systems Security.
  - reasonStorageReadOnly – база данных доступна только для чтения; необходимо восстановление Kaspersky Embedded Systems Security.

- reasonStorageIOError – ошибка ввода-вывода: а) программа Kaspersky Embedded Systems Security повреждена и нуждается в восстановлении; б) диск, на котором хранятся файлы Kaspersky Embedded Systems Security, поврежден.
- reasonStorageCorrupted – хранилище повреждено; необходимо восстановление Kaspersky Embedded Systems Security.
- reasonStorageFull – база данных заполнена; требуется свободное место на диске.
- reasonStorageOpenError – не удается открыть файл базы данных; необходимо восстановление Kaspersky Embedded Systems Security.
- reasonStorageOSFeatureError – некоторые особенности операционной системы не отвечают требованиям Kaspersky Embedded Systems Security.
- reasonObjectNotFound – помещаемый на карантин объект отсутствует на диске.
- reasonObjectAccessError – недостаточно прав для использования Backup API: учетная запись, с правами которой выполняется операция, не обладает правами Backup Operator.
- reasonDiskOutOfSpace – недостаточно места на диске.

Интеграция с WMI

Kaspersky Embedded Systems Security поддерживает интеграцию с инструментарием управления Windows (Windows Management Instrumentation, WMI): вы можете использовать клиентские системы, которые получают с помощью WMI данные по стандарту Web-Based Enterprise Management (WBEM), для получения данных о статусе программы Kaspersky Embedded Systems Security и ее компонентов.

В момент установки Kaspersky Embedded Systems Security регистрирует в системе собственный модуль для создания пространства имен Kaspersky Embedded Systems Security на защищаемом устройстве. Пространство имен Kaspersky Embedded Systems Security позволяет работать с классами, экземплярами классов и их свойствами в Kaspersky Embedded Systems Security.

Значения некоторых свойств экземпляра класса зависят от типа задачи.

Непериодические задачи – это задачи программы, которые не имеют ограниченного срока действия и либо постоянно выполняются, либо остановлены. Для таких задач невозможно указать прогресс выполнения. Результаты выполнения таких задач фиксируются непрерывно в ходе выполнения и представляют собой отдельные события (например, обнаружение зараженного объекта одной из задач постоянной защиты компьютера). Задачами такого типа можно управлять с помощью политик Kaspersky Security Center.

Периодические задачи – это задачи программы, срок выполнения которых ограничен, а прогресс выполнения может быть отображен в виде количества процентов. Результаты выполнения таких задач фиксируются по завершении задачи и представляют собой отдельный элемент или факт изменения состояния программы (например, завершение Обновления баз программы, сформированные конфигурационные файлы для задач автоматического формирования правил). На одном защищаемом устройстве одновременно может быть запущено несколько периодических задач одного типа (например, три задачи проверки по требованию с разными областями проверки). Вы можете управлять периодическими задачами с помощью групповых задач Kaspersky Security Center.

Если в вашей корпоративной сети используются инструменты, которые могут формировать запросы к пространству имен WMI и получать из него динамические данные, вы сможете получить следующие данные о текущем состоянии программы.

Свойство экземпляра класса	Описание	Значения
ProductName	Название установленной программы.	Полное название программы без номера версии.
ProductVersion	Полный номер версии установленной программы.	Полный номер версии программы, включая номер сборки.
InstalledPatches	Набор отображаемых имен установленных патчей.	Перечень критических исправлений, установленных для программы.
IsLicenseInstalled	Статус активации программы.	Статус ключа, с помощью которого активирована программа. Возможные значения: • False – В программе не добавлен лицензионный ключ. • True - В программе добавлен лицензионный ключ.
LicenseDaysLeft	Количество дней до истечения срока действия текущей лицензии.	Количество дней, оставшихся до истечения срока действия текущей лицензии. Возможные неположительные значения: • 0 - Срок действия лицензии истек. • -1 - Не удалось получить данные о текущем ключе или указанный ключ не может быть использован для активации программы (например, заблокирован по черному списку ключей).
AVBasesDatetime	Временная отметка для текущей версии антивирусных баз.	Дата и время формирования антивирусных баз, используемых в текущий момент. Если установленная программа не использует антивирусные базы, поле содержит значение Not installed.
IsExploitPreventionEnabled	Статус компонента Защита от эксплойтов.	Статус компонента Защита от эксплойтов. Возможные значения: • True - Компонент Защита от эксплойтов включен и выполняет функции защиты. • False - Компонент Защита от эксплойтов не выполняет функции защиты. Например: выключен, не установлен, нарушено Лицензионное соглашение.
ProtectionTasksRunning	Набор запущенных задач защиты.	Перечень задач защиты, контроля и мониторинга, запущенных в текущий момент. В данном поле должны учитываться все запущенные непериодические задачи. Если не запущена ни одна из непериодических задач, поле содержит значение "Нет".

IsAppControlRunning	Статус выполнения задачи Контроль запуска программ.	Статус выполнения задачи Контроль запуска программ. • True - Задача Контроль запуска программ выполняется в текущий момент. • False - Задача Контроль запуска программ не выполняется в текущий момент или компонент Контроль запуска программ не установлен.
AppControlMode	Режим работы задачи Контроль запуска программ.	Описание текущего состояния компонента Контроль запуска программ, а также выбранного режима соответствующей задачи. Возможные значения: • Active - в параметрах задачи указан режим **Активный**. • Statistics Only - в параметрах задачи указан режим **Только статистика**. • Not installed - Компонент Контроль запуска программ не установлен.
AppControlRulesNumber	Общее количество правил контроля запуска программ.	Количество правил, заданных в параметрах задачи Контроль запуска программ в текущий момент.
AppControlLastBlocking	Временная отметка последней блокировки запуска программы, выполненной задачей Контроль запуска программ в любом режиме.	Дата и время последней блокировки запуска программы, выполненной компонентом Контроль запуска программ. При заполнении поля учитываются все блокировки программ, независимо от режима выполнения задачи. Если на момент выполнения запроса WMI не зарегистрировано ни одного случая блокировки запуска программы, в поле отображается значение "Нет".
PeriodicTasksRunning	Набор запущенных периодических задач.	Перечень задач проверки по требованию, обновления и инвентаризации, запущенных в текущий момент. В данном поле должны отображаться все запущенные периодические задачи. Если не запущена ни одна из периодических задач, поле содержит значение "Нет".
ConnectionState	Состояние соединения между компонентом Поставщик WMI и службой Kaspersky Security (KAVFS).	Информация о статусе соединения между компонентом Поставщик WMI и службой Kaspersky Security. Возможные значения: • Success - Соединение успешно установлено: клиент WMI может принимать данные о статусе программы. • Failed. Error Code: <code> - Соединение не удалось установить из-за ошибки с указанным кодом.

Указанные данные являются свойствами экземпляра класса KasperskySecurity_ProductInfo.ProductName=Kaspersky Embedded Systems Security, где

- KasperskySecurity_ProductInfo – имя класса Kaspersky Embedded Systems Security.
- .ProductName=Kaspersky Embedded Systems Security – ключевое свойство Kaspersky Embedded Systems Security.

Экземпляр класса создается в пространстве имен ROOT\Kaspersky\Security.

Работа с Kaspersky Embedded Systems Security из командной строки

Этот раздел содержит описание работы с Kaspersky Embedded Systems Security из командной строки.

Команды

Вы можете выполнять основные команды управления Kaspersky Embedded Systems Security из командной строки защищаемого устройства, если при установке Kaspersky Embedded Systems Security вы включили компонент Утилита командной строки в список устанавливаемых.

С помощью командной строки можно управлять только функциями, доступными вам в соответствии с вашими правами в Kaspersky Embedded Systems Security.

Некоторые из команд Kaspersky Embedded Systems Security выполняются в следующих режимах:

- Синхронный режим: управление возвращается на Консоль только после завершения выполнения команды.
- Асинхронный режим: управление возвращается на Консоль сразу после запуска команды.

Чтобы прервать выполнение команды в синхронном режиме,

нажмите комбинацию клавиш **CTRL+C**.

При вводе команд Kaspersky Embedded Systems Security применяйте следующие правила:

- Вводите ключи и команды символами верхнего или нижнего регистра.
- Разделяйте ключи символом пробела.
- Если имя файла или папки содержит пробел, заключите путь к файлу или папке в кавычки, например: `"C:\TEST\test cpp.exe"`.
- При необходимости можно использовать подстановочные символы в масках имен файлов или путей, например: `"C:\Temp\Temp*\"`, `"C:\Temp\Temp???.doc"`, `"C:\Temp\Temp*.doc"`.

С помощью командной строки можно выполнять все операции по управлению и администрированию Kaspersky Embedded Systems Security (см. таблицу ниже).

Команды Kaspersky Embedded Systems Security

Команда	Описание
KAVSHELL APPCONTROL	Обновляет список правил в соответствии с выбранным правилом импорта.
KAVSHELL APPCONTROL /CONFIG	Задает режим работы задачи Контроль запуска программ.
KAVSHELL APPCONTROL /GENERATE	Запускает задачу Формирование правил контроля запуска программ.
KAVSHELL VACUUM	Дефрагментирует файлы журналов Kaspersky Embedded Systems Security.

KAVSHELL PASSWORD	Управляет параметрами защиты паролем.
KAVSHELL HELP	Отображает справку о командах Kaspersky Embedded Systems Security.
KAVSHELL START	Запускает службу Kaspersky Security.
KAVSHELL STOP	Останавливает службу Kaspersky Security.
KAVSHELL SCAN	Создает и запускает временную задачу проверки по требованию с областью проверки и параметрами безопасности, заданными ключами командной строки.
KAVSHELL SCANCRITICAL	Запускает системную задачу Проверка важных областей.
KAVSHELL TASK	Запускает, приостанавливает, возобновляет, останавливает указанную задачу в асинхронном режиме. Возвращает текущее состояние задачи / статистику задачи.
KAVSHELL RTP	Запускает или останавливает все задачи постоянной защиты компьютера.
KAVSHELL UPDATE	Запускает задачу Обновление баз программы с параметрами, заданными ключами командной строки.
KAVSHELL ROLLBACK	Откатывает базы программы до предыдущей версии.
KAVSHELL LICENSE	Добавляет или удаляет ключи. Отображает информацию о добавленных ключах.
KAVSHELL TRACE	Включает или выключает запись журналов трассировки. Управляет параметрами журналов трассировки.
KAVSHELL DUMP	Включает и выключает создание файлов дампов процессов Kaspersky Embedded Systems Security при их аварийном завершении.
KAVSHELL IMPORT	Импортирует общие параметры Kaspersky Embedded Systems Security, а также параметры функций и задач из конфигурационного файла.
KAVSHELL EXPORT	Экспортирует все параметры Kaspersky Embedded Systems Security и существующих задач в конфигурационный файл.
KAVSHELL DEVCONTROL	Дополняет список сформированных правил контроля устройств в соответствии с выбранным принципом добавления.

Вызов справки о командах Kaspersky Embedded Systems Security: KAVSHELL HELP

Чтобы получить список всех команд Kaspersky Embedded Systems Security, выполните одну из следующих команд:

```
KAVSHELL

KAVSHELL HELP

KAVSHELL /?
```

Чтобы получить описание команды и ее синтаксис, выполните одну из следующих команд:

```
KAVSHELL HELP <команда>
```

```
KAVSHELL <команда> /?
```

Примеры команды KAVSHELL HELP

Чтобы просмотреть подробную информацию о команде KAVSHELL SCAN, выполните следующую команду:

```
KAVSHELL HELP SCAN
```

Запуск и остановка службы Kaspersky Security. KAVSHELL START, KAVSHELL STOP

Чтобы запустить службу Kaspersky Security, выполните следующую команду:

```
KAVSHELL START
```

По умолчанию при запуске службы Kaspersky Security запускается Постоянная защита файлов и Проверка при старте операционной системы, а также другие задачи, в расписании которых указана частота **При запуске программы**.

Чтобы остановить службу Kaspersky Security, выполните следующую команду:

```
KAVSHELL STOP
```

Для выполнения команды может потребоваться ввод пароля. Для ввода текущего пароля используйте ключ `[/pwd:<пароль>]`.

Проверка выбранной области. KAVSHELL SCAN

Чтобы запустить задачу проверки отдельных областей защищаемого устройства, используйте команду `KAVSHELL SCAN`. Ключи этой команды задают параметры области проверки и параметры безопасности выбранного узла.

Задача проверки по требованию, запущенная с помощью команды `KAVSHELL SCAN`, является временной. Она отображается в Консоли программы только во время выполнения (в Консоли программы не отображаются ее параметры). Однако в узле **Журналы выполнения задач** в Консоли программы формируется и отображается журнал выполнения задачи.

При указании путей в задачах проверки отдельных областей можно использовать переменные окружения. Если вы используете переменную окружения, назначенную для пользователя, выполните команду `KAVSHELL SCAN` с правами этого пользователя.

Команда `KAVSHELL SCAN` выполняется в синхронном режиме.

Чтобы запустить из командной строки существующую задачу проверки по требованию, используйте команду KAVSHELL TASK.

Синтаксис команды KAVSHELL SCAN

```
KAVSHELL SCAN <области проверки> [/MEMORY|/SHARED|/STARTUP|/REMDRIVES|/FIXDRIVES|/MYCOMP]
[/L:<имя файла со списком областей проверки>] [/F<A|C|E>] [/NEWONLY] [/AI:
<DISINFECT|DISINFDEL|DELETE|REPORT|AUTO>] [/AS:<QUARANTINE|DELETE|REPORT|AUTO>]
[/DISINFECT|/DELETE] [/E:<ABMSPO>] [/EM:<"маски">] [/ES:<размер>] [/ET:<количество
секунд>] [/TZOFF] [/OF:<SKIP|RESIDENT|SCAN[=<дни>] [NORECALL]>] [/NOICHECKER][/NOISWIFT]
[/ANALYZERLEVEL][/W:<имя файла журнала выполнения задачи>] [/ANSI] [/ALIAS:
<альтернативное название задачи>]
```

У команды KAVSHELL SCAN есть обязательные и дополнительные ключи/параметры (см. таблицу ниже).

Примеры команды KAVSHELL SCAN

```
KAVSHELL SCAN Folder56 D:\Folder1\Folder2\Folder3\ C:\Folder1\ C:\Folder2\3.exe
"\\another server\Shared\" F:\123\*.fgb /SHARED /AI:DISINFDEL /AS:QUARANTINE /FA /E:ABM
/EM:"*.xtx;*.fff;*.ggg;*.bbb;*.info" /NOICHECKER /ANALYZERLEVEL:1 /NOISWIFT /W:log.log

KAVSHELL SCAN /L:scan_objects.lst /W:c:\log.log
```

Ключи / параметры команды KAVSHELL SCAN

Ключ / параметр	Описание
Область проверки. Обязательный параметр.	
<файлы> <папки> <сетевой путь>	Область проверки – список файлов, папок, сетевых путей и стандартных областей. Указывайте сетевые пути к формате UNC (Universal Naming Convention). В следующем примере папка Folder4 указана без пути к ней. Это значит, что она находится в папке, из которой вы запускаете команду KAVSHELL. KAVSHELL SCAN Folder4 Если имя объекта, который вы хотите проверить, содержит пробелы, заключайте его в кавычки. Kaspersky Embedded Systems Security проверит также все вложенные папки в выбранной папке. Для проверки группы файлов вы можете использовать символы * или ?.
/MEMORY	Проверять объекты в оперативной памяти.
/SHARED	Проверять папки общего доступа на защищаемом устройстве.
/STARTUP	Проверять объекты автозапуска.
/REMDRIVES	Проверять съемные диски.
/FIXDRIVES	Проверять жесткие диски.
/MYCOMP	Проверять все области защищаемого устройства.
/L: <путь к файлу со списком областей проверки>	Полный путь к файлу со списком областей проверки. Разделяйте области проверки в файле символом перевода строки. Вы можете указывать стандартные области проверки, как показано в следующем примере файла со списком областей проверки: C:\ D:\Docs*.doc E:\My Documents

	/STARTUP /SHARED
Проверка объектов (типы файлов). Если вы не укажете этот ключ, Kaspersky Embedded Systems Security будет проверять объекты по формату.	
/FA	Проверять все объекты
/FC	Проверять объекты по формату (по умолчанию). Kaspersky Embedded Systems Security проверяет только объекты, форматы которых входят в список форматов, свойственных заражаемым объектам.
/FE	Проверять объекты по расширению. Kaspersky Embedded Systems Security проверяет только объекты с расширениями, которые входят в список расширений, свойственных заражаемым объектам.
/NEWONLY	Проверять только новые и измененные файлы. Если вы не укажете этот ключ, Kaspersky Embedded Systems Security будет проверять все объекты.
Действия над зараженными и другими обнаруженными объектами. Если вы не зададите никаких значений этого ключа, Kaspersky Embedded Systems Security будет выполнять действие **Пропускать**.	
DISINFECT	Лечить; если лечение невозможно, пропускать Параметры DISINFECT и DELETE сохранены в текущей версии Kaspersky Embedded Systems Security для обеспечения совместимости с предыдущими версиями. Эти параметры можно использовать вместо параметров /AI и /AS. В этом случае Kaspersky Embedded Systems Security не будет обрабатывать возможно зараженные объекты.
DISINFDEL	Лечить; если лечение невозможно, удалять
DELETE	Удалять Параметры DISINFECT и DELETE сохранены в текущей версии Kaspersky Embedded Systems Security для обеспечения совместимости с предыдущими версиями. Эти параметры можно использовать вместо параметров /AI и /AS. В этом случае Kaspersky Embedded Systems Security не будет обрабатывать возможно зараженные объекты.
REPORT	Отсылать отчет (по умолчанию)
AUTO	Выполнять рекомендованное действие
/AS: **Действия над возможно зараженными объектами**. Если вы не укажете этот параметр, Kaspersky Embedded Systems Security будет выполнять действие **Пропускать**.	
QUARANTINE	Карантин
DELETE	Удалять
REPORT	Отсылать отчет (по умолчанию)
AUTO	Выполнять рекомендованное действие
Исключения	
/E:ABMSPO	Исключать составные объекты следующих типов: A – SFX-архивы; B – почтовые базы; M – файлы почтовых форматов; S – архивы (включая SFX-архивы); P – упакованные объекты;

	O – вложенные OLE-объекты.
/EM:<"маски">	Исключать файлы по маске Можно указать несколько масок, например: EM: " *.txt; *.png; C\Videos*.avi " .
/ET:<количество секунд>	Прекращать обработку объекта, если она продолжается дольше указанного количества секунд. По умолчанию ограничений продолжительности нет.
/ES:<размер>	Исключать из проверки составные объекты, размер которых в мегабайтах превышает указанное значение. По умолчанию Kaspersky Embedded Systems Security проверяет объекты любого размера.
/TZOFF	Отменить исключения доверенной зоны.
Дополнительные параметры (опции)	
/NOICHECKER	Выключить использование технологии iChecker (по умолчанию включено).
/NOISWIFT	Выключить использование технологии iSwift (по умолчанию включено).
/ANALYZERLEVEL:<уровень эвристического анализа>	Включить использование эвристического анализатора, настроить уровень анализа. Доступны следующие уровни эвристического анализа: 1 – поверхностный; 2 – средний; 3 – глубокий. Если вы опустите этот параметр, Kaspersky Embedded Systems Security не будет использовать эвристический анализатор.
/ALIAS:<альтернативное название задачи>	Присваивает задаче проверки по требованию временное название, по которому к задаче можно обращаться во время ее выполнения, например, чтобы просмотреть ее статистику с помощью команды TASK. Альтернативное название задачи должно быть уникальным среди альтернативных названий задач всех компонентов Kaspersky Embedded Systems Security. Если этот параметр не задан, задаче присваивается временное название вида scan_<kavshell_pid>, например, scan_1234. В Консоли программы задаче присваивается название "Проверка объектов <дата и время>", например, "Проверка объектов 16.08.2007 17:13:14".
Параметры журнала выполнения задачи	
/W:<имя файла журнала выполнения задачи>	Если указан этот параметр, Kaspersky Embedded Systems Security сохранит файл журнала выполнения задачи с именем, заданным значением параметра. Файл журнала содержит статистику выполнения задачи, время ее запуска и завершения (остановки), а также информацию о событиях задачи. В журнале регистрируются события, заданные параметрами журнала выполнения задачи и параметрами журнала событий Kaspersky Embedded Systems Security в оснастке "Просмотр событий". Вы можете указать абсолютный или относительный путь к файлу журнала. Если вы укажете только имя файла, не указав путь к нему, файл журнала будет создан в текущей папке. Повторный запуск команды с теми же параметрами записи в журнал перезаписывает существующий файл журнала. Вы можете просматривать файл журнала во время выполнения задачи. Журнал отображается в узле Журналы выполнения задач Консоли программы.

	Если Kaspersky Embedded Systems Security не удается создать файл журнала, выполнение команды не прерывается, а выдается сообщение об ошибке.
/ANSI	Этот параметр позволяет записывать события в журнал выполнения задачи в кодировке ANSI. Параметр ANSI не будет применяться, если не задан параметр W. Если параметр ANSI не указан, то журнал выполнения задачи формируется в кодировке UNICODE.

Запуск задачи Проверка важных областей. KAVSHELL SCANCRITICAL

Используйте команду `KAVSHELL SCANCRITICAL`, чтобы запустить задачу Проверка важных областей с параметрами, заданными в Консоли программы.

Синтаксис команды KAVSHELL SCANCRITICAL

```
KAVSHELL SCANCRITICAL [/W:<имя файла журнала выполнения задачи>]
```

Примеры команды KAVSHELL SCANCRITICAL

Чтобы запустить задачу Проверка важных областей и сохранить журнал выполнения задачи в файле с именем scancritical.log в текущей папке, выполните следующую команду:

```
KAVSHELL SCANCRITICAL /W:scancritical.log
```

С помощью параметра /W можно настроить местоположение файла журнала выполнения задачи (см. таблицу ниже).

Синтаксис параметра `/W` команды `KAVSHELL SCANCRITICAL`

Ключ / параметр	Описание
/W:<имя файла журнала выполнения задачи>	Если указан этот параметр, Kaspersky Embedded Systems Security сохранит файл журнала выполнения задачи с именем, заданным значением параметра. Файл журнала содержит статистику выполнения задачи, время ее запуска и завершения (остановки), а также информацию о событиях задачи. В журнале регистрируются события, заданные параметрами журнала выполнения задачи и параметрами журнала событий Kaspersky Embedded Systems Security в оснастке "Просмотр событий". Вы можете указать абсолютный или относительный путь к файлу журнала. Если вы укажете только имя файла, не указав путь к нему, файл журнала будет создан в текущей папке. Повторный запуск команды с теми же параметрами записи в журнал перезаписывает существующий файл журнала. Вы можете просматривать файл журнала во время выполнения задачи. Журнал отображается в узле **Журналы выполнения задач** в Консоли программы. Если Kaspersky Embedded Systems Security не удается создать файл журнала, выполнение команды не прерывается, а выдается сообщение об ошибке.

Управление задачей в асинхронном режиме. KAVSHELL TASK

Команда KAVSHELL TASK позволяет управлять указанной задачей: запускать, приостанавливать, возобновлять и останавливать задачу, а также просматривать ее текущее состояние и статистику. Команда выполняется в асинхронном режиме.

Для выполнения команды может потребоваться ввод пароля. Для ввода текущего пароля используйте ключ [/pwd:<пароль>].

Синтаксис команды KAVSHELL TASK

```
KAVSHELL TASK [<альтернативное название задачи> </START | /STOP | /PAUSE | /RESUME | /STATE | /STATISTICS>]
```

Примеры команды KAVSHELL TASK

```
KAVSHELL TASK

KAVSHELL TASK on-access /START

KAVSHELL TASK user-task_1 /STOP

KAVSHELL TASK scan-computer /STATE

KAVSHELL TASK network-attack-blocker /START
```

Команда KAVSHELL TASK может быть выполнена как без ключей/параметров, так и с использованием одного либо нескольких ключей/параметров (см. таблицу ниже).

Ключи / параметры команды KAVSHELL TASK

Ключ / параметр	Описание
Без параметров	Возвращает список всех существующих задач Kaspersky Embedded Systems Security. Список содержит следующие поля: альтернативное название задачи, категория задачи (системная или пользовательская) и текущий статус задачи.
<альтернативное название задачи>	Вместо названия задачи в команде SCAN TASK используйте ее альтернативное название – дополнительное сокращенное название, которое Kaspersky Embedded Systems Security присваивает задачам. Чтобы просмотреть альтернативные названия задач Kaspersky Embedded Systems Security, введите команду KAVSHELL TASK без параметров.
/START	Запустить указанную задачу в асинхронном режиме
/STOP	Остановить указанную задачу
/PAUSE	Приостановить указанную задачу
/RESUME	Возобновить указанную задачу в асинхронном режиме
/STATE	Получить текущее состояние задачи (например, *Выполняется*, *Завершена*, *Приостановлена*, *Остановлена*, *Завершена с ошибкой*, *Запускается*, *Возобновляется*).

/STATISTICS	Получить статистику задачи – информацию о количестве объектов, обработанных с начала выполнения задачи

Обратите внимание, что не все задачи Kaspersky Embedded Systems Security поддерживают ключи /PAUSE, /RESUME и /STATE.

Коды возврата команды KAVSHELL TASK.

Удаление атрибута защищенного процесса (PPL): KAVSHELL CONFIG

Команда `KAVSHELL CONFIG` позволяет удалить атрибут защищенного процесса (Protected Process Light) у службы Kaspersky Security с помощью драйвера ELAM, установленного во время установки программы.

Синтаксис команды KAVSHELL CONFIG

```
KAVSHELL CONFIG /PPL:<OFF>
```

Ключи / параметры команды KAVSHELL CONFIG

Ключ / параметр	Описание
/PPL:OFF	Снять атрибут PPL со службы Kaspersky Security.

Запуск и остановка задач постоянной защиты компьютера. KAVSHELL RTP

Команда `KAVSHELL RTP` позволяет запустить или остановить все задачи постоянной защиты компьютера.

Для выполнения команды может потребоваться ввод пароля. Для ввода текущего пароля используйте ключ `[/pwd:<пароль>]`.

Синтаксис команды KAVSHELL RTP

```
KAVSHELL RTP </START | /STOP>
```

Примеры команды KAVSHELL RTP

Чтобы запустить все задачи постоянной защиты компьютера, выполните следующую команду:

```
KAVSHELL RTP /START
```

Команда `KAVSHELL RTP` должна включать один из двух параметров (см. таблицу ниже).

Параметры команды KAVSHELL RTP

Ключ /	Описание

параметр	
/START	Запустить все задачи постоянной защиты компьютера: Постоянная защита файлов и Использование KSN.
/STOP	Остановить все задачи постоянной защиты компьютера.

Управление задачей Контроль запуска программ. KAVSHELL APPCONTROL /CONFIG

Команда `KAVSHELL APPCONTROL /CONFIG` позволяет настраивать режим работы задачи Контроль запуска программ и контролировать загрузку DLL-модулей.

Синтаксис команды KAVSHELL APPCONTROL /CONFIG

```
/config /mode:<applyrules|statistics> [/dll:<no|yes>] | /config /savetofile:<полный путь к XML файлу>
```

Примеры команды KAVSHELL APPCONTROL /CONFIG

*Чтобы запустить задачу Контроль запуска программ в режиме **Активный** без контроля загрузки DLL-модулей и сохранить параметры задачи по завершении, выполните следующую команду:*

```
KAVSHELL APPCONTROL /CONFIG /mode:applyrules /dll:<no>
/savetofile:c:\appcontrol\config.xml
```

Вы можете настраивать параметры задачи Контроль запуска программ с помощью ключей (см. таблицу ниже).

Ключи / параметры команды `KAVSHELL APPCONTROL /CONFIG`

Ключ / параметр	Описание
`/mode:<applyrules|statistics>`	Режим работы задачи Контроль запуска программ. Вы можете выбрать один из следующих режимов работы задачи: • active - применяются правила контроля запуска программ; • statistics - только формировать статистику.
`/dll:<no|yes>`	Выключить или включить контроль загрузки DLL-модулей.
`/savetofile: <путь к xml-файлу>`	Экспортировать заданные правила в указанный файл в формате XML.
`/savetofile: <полное имя xml-файла>`	Сохранить список правил в файл.
`/savetofile: <полное имя xml-файла> /sdc`	Сохранить список правил контроля распространения программного обеспечения в файл.
`/clearsdc`	Удалить все правила контроля распространения программного обеспечения.

Формирование правил контроля запуска программ. KAVSHELL APPCONTROL /GENERATE

Команда `KAVSHELL APPCONTROL /GENERATE` позволяет формировать списки правил контроля запуска программ.

Для выполнения команды может потребоваться ввод пароля. Для ввода текущего пароля используйте ключ `[/pwd:<пароль>]`.

Синтаксис команды KAVSHELL APPCONTROL /GENERATE

```
KAVSHELL APPCONTROL /GENERATE <путь к папке> | /source:<путь к файлу со списком папок>
[/masks:<edms>] [/runapp] [/rules:<ch|cp|h>] [/strong] [/user:<пользователь или группа
пользователей>] [/export:<полный путь к XML файлу>] [/import:<a|r|m>] [/prefix:<префикс
для названий правил>] [/unique]
```

Примеры команды KAVSHELL APPCONTROL /GENERATE

Чтобы сформировать правила для файлов из указанных папок, выполните команду:

```
KAVSHELL APPCONTROL /GENERATE /source:c\folderslist.txt
/export:c:\rules\appctrlrules.xml
```

Чтобы сформировать правила для исполняемых файлов с любыми расширениями, хранящихся в указанной папке, и по завершении задачи сохранить сформированные правила в указанный XML-файл, выполните следующую команду:

```
KAVSHELL APPCONTROL /GENERATE c:\folder /masks:edms /export:c\rules\appctrlrules.xml
```

Вы можете использовать ключи/параметры для настройки автоматического формирования правил задачи Контроль запуска программ (см. таблицу ниже).

Ключи / параметры команды `KAVSHELL APPCONTROL /GENERATE`

Ключ / параметр	Описание
Область применения разрешающих правил	
<путь к папке>	Указать путь к папке с исполняемыми файлами, для которых будут автоматически формироваться разрешающие правила.
/source: <путь к файлу со списком папок>	Указать путь к TXT-файлу со списком папок, содержащих исполняемые файлы, для которых будут автоматически формироваться разрешающие правила.
/masks: <edms>	Указать расширения исполняемых файлов, для которых будут автоматически формироваться разрешающие правила. В область применения правил можно включить файлы со следующими расширениями: • e - файлы с расширением exe;

	• d - файлы с расширением dll; • m - файлы с расширением msi; • s - скрипты.
/runapp	Учитывать при формировании разрешающих правил программы, запущенные на защищаемом устройстве в текущий момент.
Действия при автоматическом формировании разрешающих правил	
/rules: <ch|cp|h>	Указать действия при формировании разрешающих правил для задачи Контроль запуска программ: • ch – использовать цифровой сертификат. Если сертификат отсутствует, использовать SHA256-хеш. • cp — использовать цифровой сертификат. Если сертификат отсутствует, использовать путь к исполняемому файлу. • h – использовать SHA256-хеш.
/strong	Использовать заголовок и отпечаток цифрового сертификата при автоматическом формировании разрешающих правил для задачи Контроль запуска программ. Команда выполняется, если указан параметр /rules: <ch|cp>.
/user: <пользователь или группа пользователей>	Указать имя пользователя или группы пользователей, для которых должны применяться правила. Программа будет контролировать запуски программ указанным пользователем и / или группой.
Действия по завершении выполнения задачи Формирование правил контроля запуска программ	
/export: <путь к XML-файлу>	Сохранить сформированные правила в XML-файл.
/unique	Добавлять информацию о защищаемом устройстве, по программам которого формируются разрешающие правила контроля запуска программ.
/prefix: <префикс для названий правил>	Указать префикс названий разрешающих правил контроля запуска программ.
/import: <a|r|m>	Импортировать сформированные правила в указанный список правил контроля запуска программ в соответствии с выбранным принципом добавления новых правил: • a – **Добавить правила к существующим** (одинаковые правила дублируются); • r – **Заменить существующие правила** (правила с одинаковыми параметрами не добавляются; правило добавляется, если хотя бы один параметр правила уникален); • m – **Объединить правила с существующими** (правила с одинаковыми параметрами не добавляются; правило добавляется, если хотя бы один параметр правила уникален).

Наполнение списка правил контроля запуска программ. KAVSHELL APPCONTROL

Команда `KAVSHELL APPCONTROL` позволяет добавлять правила из XML-файла в список правил задачи Контроль запуска программ в соответствии с выбранным принципом, а также удалять все правила из списка.

Для выполнения команды может потребоваться ввод пароля. Для ввода текущего пароля используйте ключ `[/pwd:<пароль>]`.

Синтаксис команды KAVSHELL APPCONTROL

```
KAVSHELL APPCONTROL /append <полный путь к XML файлу> | /replace <полный путь к XML файлу> | /merge <полный путь к XML файлу> | /clear
```

Пример команды KAVSHELL APPCONTROL

Чтобы добавить к имеющимся правилам контроля запуска программ правила из XML-файла по принципу Добавить к существующим правилам, выполните команду:

```
KAVSHELL APPCONTROL /append c:\rules\appctrlrules.xml
```

С помощью параметров командной строки можно выбрать принцип добавления новых правил из указанного XML-файла в заданный список правил контроля запуска программ (см. таблицу ниже).

Ключи / параметры команды `KAVSHELL APPCONTROL`

Ключ / параметр	Описание
/append <полный путь к XML файлу>	Дополнить список правил контроля запуска программ правилами из указанного XML-файла. Правило импорта – **Добавить правила к существующим** (одинаковые правила дублируются).
/replace <полный путь к XML файлу>	Дополнить список правил контроля запуска программ правилами из указанного XML-файла. Правило импорта – **Заменить существующие правила** (правила с одинаковыми параметрами не добавляются; правило добавляется, если хотя бы один параметр правила уникален).
/merge <полный путь к XML файлу>	Дополнить список правил контроля запуска программ правилами из указанного XML-файла. Правило импорта – **Объединить правила с существующими** (новые правила не дублируют существующие правила).
/clear	Очистить список правил контроля запуска программ.

Наполнение списка правил контроля устройств. KAVSHELL DEVCONTROL

Команда `KAVSHELL DEVCONTROL` позволяет добавлять правила из XML-файла в список правил задачи Контроль устройств в соответствии с выбранным принципом, а также удалять все правила из списка.

Для выполнения команды может потребоваться ввод пароля. Для ввода текущего пароля используйте ключ `[/pwd:<пароль>]`.

Синтаксис команды KAVSHELL DEVCONTROL

```
KAVSHELL DEVCONTROL /append <полный путь к XML файлу> | /replace <полный путь к XML файлу> | /merge <полный путь к XML файлу> | /clear
```

Пример команды KAVSHELL DEVCONTROL

Чтобы добавить к имеющимся правилам контроля устройств правила из XML-файла по принципу Добавить к существующим правилам, выполните команду:

```
KAVSHELL DEVCONTROL /append :c:\rules\devctrlrules.xml
```

С помощью параметров командной строки можно выбрать принцип добавления новых правил из указанного XML-файла в заданный список правил контроля устройств (см. таблицу ниже).

Ключи / параметры команды `KAVSHELL DEVCONTROL`

Ключ	Описание
/append <полный путь к XML файлу>	Дополнить список правил контроля устройств правилами из указанного XML-файла. Правило импорта – **Добавить правила к существующим** (одинаковые правила дублируются).
/replace <полный путь к XML файлу>	Дополнить список правил контроля устройств правилами из указанного XML-файла. Правило импорта – **Заменить существующие правила** (правила с одинаковыми параметрами не добавляются; правило добавляется, если хотя бы один параметр правила уникален).
/merge <полный путь к XML файлу>	Дополнить список правил контроля устройств правилами из указанного XML-файла. Правило импорта – **Объединить правила с существующими** (новые правила не дублируют существующие правила).
/clear	Очистить список правил контроля устройств.

Запуск задачи Обновление баз программы. KAVSHELL UPDATE

Команда KAVSHELL UPDATE позволяет запускать задачу обновления баз Kaspersky Embedded Systems Security в синхронном режиме.

Задача Обновление баз программы, запущенная с помощью команды KAVSHELL UPDATE, является временной. Она отображается в Консоли программы только во время ее выполнения. Однако в узле **Журналы выполнения задач** в Консоли программы формируется и отображается журнал выполнения задачи. К задачам обновления, созданным и запущенным с помощью команды KAVSHELL UPDATE, и к задачам обновления, созданным в Консоли программы, могут применяться политики Kaspersky Security Center. Сведения об использовании Kaspersky Security Center для управления Kaspersky Embedded Systems Security на защищаемых устройствах приведены в разделе "Управление Kaspersky Embedded Systems Security с помощью Kaspersky Security Center".

Чтобы указать путь к источнику обновлений в этой задаче, можно использовать переменные окружения. Если вы используете переменную окружения, назначенную для пользователя, выполните команду KAVSHELL UPDATE с правами этого пользователя.

Синтаксис команды KAVSHELL UPDATE

```
KAVSHELL UPDATE <Путь к источнику обновления | /AK | /KL> [/NOUSEKL] [/PROXY:<адрес>:
<порт>] [/AUTHTYPE:<0-2>] [/PROXYUSER:<имя пользователя>] [/PROXYPWD:<пароль>]
[/NOPROXYFORKL] [/USEPROXYFORCUSTOM] [/USEPROXYFORLOCAL] [/NOFTPPASSIVE] [/TIMEOUT:
<количество секунд>] [/REG:<код iso3166>] [/W:<имя файла журнала выполнения задачи>]
[/ALIAS:<альтернативное название задачи>]
```

У команды KAVSHELL UPDATE есть обязательные и дополнительные ключи/параметры (см. таблицу ниже).

Пример команды KAVSHELL UPDATE

Чтобы запустить пользовательскую задачу Обновление баз программы, выполните следующую команду:

```
KAVSHELL UPDATE
```

Чтобы запустить задачу Обновление баз программы, файлы обновлений для которой хранятся в сетевой папке \\server\databases, выполните следующую команду:

```
KAVSHELL UPDATE \\server\bases
```

Чтобы запустить задачу Обновление баз программы с FTP-сервера ftp://dnl-ru1.kaspersky-labs.com/ и записать все события задачи в файл c:\update_report.log, выполните следующую команду:

```
KAVSHELL UPDATE ftp://dnl-ru1.kaspersky-labs.com /W:c:\update_report.log
```

Чтобы загрузить обновления баз Kaspersky Embedded Systems Security с сервера обновлений "Лаборатории Касперского", подключитесь к источнику обновлений с помощью прокси-сервера (адрес прокси-сервера: proxy.company.com, порт: 8080). Для доступа к защищаемому устройству с помощью встроенной в Windows проверки подлинности NTLM с именем пользователя netuser и паролем 123456, выполните следующую команду:

```
KAVSHELL UPDATE /KL /PROXY:proxy.company.com:8080 /AUTHTYPE:1 /PROXYUSER:inetuser
/PROXYPWD:123456
```

Ключи / параметры команды KAVSHELL UPDATE

Ключ / параметр	Описание

Источник обновлений (обязательный параметр). Укажите один или несколько источников. Kaspersky Embedded Systems Security будет обращаться к источникам в порядке их перечисления. Разделяйте источники символом пробела.	
<путь в формате UNC>	Пользовательские источники обновления. Путь к сетевой папке с обновлениями в формате UNC.
<URL>	Пользовательские источники обновления. Адрес HTTP- или FTP-сервера, на котором располагается папка с обновлениями.
<Локальная папка>	Пользовательские источники обновления. Папка на защищаемом устройстве.
/AK	Использовать Сервер администрирования Kaspersky Security Center в качестве источника обновлений.
/KL	Использовать серверы обновлений "Лаборатории Касперского" в качестве источника обновлений.
/NOUSEKL	Не использовать серверы обновлений "Лаборатории Касперского", если другие источники обновлений недоступны (по умолчанию).
Параметры прокси-сервера	
/PROXY:<адрес>:<порт>	Сетевое имя или IP-адрес прокси-сервера и его порт. Если вы не укажете этот параметр, Kaspersky Embedded Systems Security будет автоматически распознавать параметры прокси-сервера, который используется в локальной сети.
/AUTHTYPE:<0-2>	Этот параметр задает метод аутентификации для доступа к прокси-серверу. Он может принимать следующие значения: **0** – проверка подлинности NTLM в Microsoft Windows; Kaspersky Embedded Systems Security обращается к прокси-серверу с использованием учетной записи **Локальная система** (**SYSTEM**). **1** – проверка подлинности NTLM в Microsoft Windows; Kaspersky Embedded Systems Security обращается к прокси-серверу с использованием учетной записи, имя пользователя и пароль которой заданы параметрами /PROXYUSER и /PROXYPWD. **2** – обычная проверка подлинности по имени пользователя и паролю, заданным параметрами /PROXYUSER и /PROXYPWD. Если для доступа к прокси-серверу не требуется аутентификация, можно не указывать этот параметр.
/PROXYUSER:<имя пользователя>	Имя пользователя, используемое для доступа к прокси-серверу. Если указано значение /AUTHTYPE:0, то параметры /PROXYUSER:<имя пользователя> и /PROXYPWD:<пароль> игнорируются.
/PROXYPWD:<пароль>	Пароль пользователя, используемый для доступа к прокси-серверу. Если указано значение /AUTHTYPE:0, то параметры /PROXYUSER:<имя пользователя> и /PROXYPWD:<пароль> игнорируются. Если указан параметр /PROXYUSER, но не указан параметр /PROXYPWD, считается, что задан пустой пароль.
/NOPROXYFORKL	Не использовать параметры прокси-сервера для соединения с серверами обновлений "Лаборатории Касперского" (по умолчанию).
/USEPROXYFORCUSTOM	Использовать параметры прокси-сервера для соединения с пользовательскими источниками обновлений (по умолчанию не используется).
/USEPROXYFORLOCAL	Использовать параметры прокси-сервера для соединения с локальными источниками обновлений. Если не указано, применяется значение **Не использовать прокси-сервер для локальных адресов**.

Общие параметры FTP- и HTTP-сервера	
/NOFTPPASSIVE	Если указан этот ключ, Kaspersky Embedded Systems Security использует активный режим FTP-сервера для соединения с защищаемым устройством. Если вы не укажете этот ключ, Kaspersky Embedded Systems Security использует пассивный режим FTP-сервера, при возможности.
/TIMEOUT:<количество секунд>	Время ожидания при соединении с FTP- или HTTP-сервером. Если вы не укажете этот параметр, Kaspersky Embedded Systems Security использует значение по умолчанию: 10 секунд. Значение параметра должно быть целым числом.
/REG:<код iso3166>	Региональные параметры. Этот параметр используется при получении обновлений с серверов обновлений Лаборатории Касперского". Kaspersky Embedded Systems Security минимизирует нагрузку на защищаемое устройство, выбирая ближайший к нему сервер обновлений. Значение этого параметра должно быть двухбуквенным кодом страны, в которой расположено защищаемое устройство, в стандарте ISO 3166-1, например: /REG: gr или /REG:US. Если ключ не указан или указан недопустимый код страны, Kaspersky Embedded Systems Security распознает местоположение защищаемого устройства в соответствии с региональными параметрами защищаемого устройства, на котором установлена Консоль программы.
/ALIAS:<альтернативное название задачи>	Этот параметр позволяет присвоить задаче временное имя, по которому к ней можно обращаться во время ее выполнения. Например, вы можете просмотреть статистику задачи с помощью команды TASK. Альтернативное название задачи должно быть уникальным среди альтернативных названий задач всех компонентов Kaspersky Embedded Systems Security. Если этот ключ не задан, задаче присваивается временное название вида update_<kavshell_pid>, например, update_1234. В Консоли программы задаче присваивается название "Обновление баз программы <дата и время>", например: "Обновление баз программы 16.08.2007 17:41:02".
/W:<имя файла журнала выполнения задачи>	Если указан этот параметр, Kaspersky Embedded Systems Security сохранит файл журнала выполнения задачи с именем, заданным значением параметра. Файл журнала содержит статистику выполнения задачи, время ее запуска и завершения (остановки), а также информацию о событиях задачи. В журнале регистрируются события, заданные параметрами журнала выполнения задачи и параметрами журнала событий Kaspersky Embedded Systems Security в оснастке "Просмотр событий". Вы можете указать абсолютный или относительный путь к файлу журнала. Если вы укажете только имя файла, не указав путь к нему, файл журнала будет создан в текущей папке. Повторный запуск команды с теми же параметрами записи в журнал перезаписывает существующий файл журнала. Вы можете просматривать файл журнала во время выполнения задачи. Журнал отображается в узле **Журналы выполнения задач** в Консоли программы. Если Kaspersky Embedded Systems Security не удается создать файл журнала, выполнение команды не прерывается, а выдается сообщение об ошибке.

Коды возврата команды KAVSHELL UPDATE.

Откат обновления баз Kaspersky Embedded Systems Security. KAVSHELL ROLLBACK

Команда `KAVSHELL ROLLBACK` позволяет выполнить системную задачу Откат обновления баз программы – откатить базы Kaspersky Embedded Systems Security до предыдущей установленной версии. Команда выполняется синхронно.

Синтаксис команды

```
KAVSHELL ROLLBACK
```

Коды возврата команды KAVSHELL ROLLBACK.

Управление анализом журналов. KAVSHELL TASK LOG-INSPECTOR

Команда `KAVSHELL TASK LOG-INSPECTOR` позволяет осуществлять контроль целостности среды, основываясь на анализе журнала событий Windows.

Синтаксис команды

```
KAVSHELL TASK LOG-INSPECTOR
```

Пример команды

```
KAVSHELL TASK LOG-INSPECTOR /stop
```

Ключи / параметры команды KAVSHELL TASK LOG-INSPECTOR

Ключ / параметр	Описание
/START	Запустить указанную задачу в асинхронном режиме
/STOP	Остановить указанную задачу
/STATE	Получить текущее состояние задачи (например, *Выполняется*, *Завершена*, *Приостановлена*, *Остановлена*, *Завершена с ошибкой*, *Запускается*, *Возобновляется*).
/STATISTICS	Получить статистику задачи – информацию о количестве объектов, обработанных с начала выполнения задачи.

Коды возврата команды KAVSHELL TASK LOG-INSPECTOR.

Включение, настройка и выключение журналов трассировки. KAVSHELL TRACE

Команда `KAVSHELL TRACE` позволяет включать или выключать ведение журнала трассировки всех подсистем Kaspersky Embedded Systems Security, а также устанавливать уровень детализации информации в журнале.

Kaspersky Embedded Systems Security записывает информацию в файлы трассировки и файлы дампов в незашифрованном виде.

Синтаксис команды KAVSHELL TRACE

```
KAVSHELL TRACE </ON /F:<папка с файлами журнала трассировки> [/S:<максимальный размер файла журнала в мегабайтах>] [/LVL:debug|info|warning|error|critical] | /OFF>
```

Если ведется журнал трассировки и вы хотите изменить его параметры, введите команду `KAVSHELL TRACE` с ключом /ON и с помощью ключей /S и /LVL задайте параметры журнала трассировки (см. таблицу ниже).

Ключи / параметры команды KAVSHELL TRACE

Ключ	Описание
/ON	Включить ведение журнала трассировки.
/F:<папка с файлами журнала трассировки>	Этот параметр указывает полный путь к папке, в которую будут сохранены файлы журнала трассировки (обязательный). Если вы укажете путь к несуществующей папке, журнал трассировки не будет создан. Пути к папкам на сетевых дисках других защищаемых устройств указывать нельзя. Если указанный параметром путь содержит пробел, заключите его в кавычки, например: /F:"C:\Trace Folder". Указывая путь к папке с файлами журнала трассировки, вы можете использовать системные переменные окружения; вы не можете использовать пользовательские переменные окружения.
/S: <максимальный размер файла журнала в мегабайтах>	Этот ключ устанавливает максимальный размер одного файла журнала трассировки. Как только файл журнала достигнет максимального размера, Kaspersky Embedded Systems Security начнет записывать информацию в новый файл; предыдущий файл журнала сохранится. Если значение этого параметра не указано, максимальный размер одного файла журнала составит 50 МБ.
/LVL:debug|info|warning|error|critical	Этот параметр устанавливает уровень детализации журнала от максимального (**Вся отладочная информация**), при котором в журнал записываются все события, до минимального (**Критические события**), при котором в журнал записываются только критические события. Если значение этого параметра не указано, в журнал трассировки будут записываться все события с уровнем детализации **Вся отладочная информация**.
/OFF	Этот параметр выключает ведение журнала трассировки.

Примеры команды KAVSHELL TRACE

*Чтобы включить ведение журнала трассировки с уровнем детализации **Вся отладочная информация** и максимальным размером файла журнала 200 МБ и сохранить файл журнала в папке C:\Trace Folder, выполните команду:*

```
KAVSHELL TRACE /ON /F:"C:\Trace Folder" /S:200
```

*Чтобы включить ведение журнала трассировки с уровнем детализации **Важные события** и сохранить файл журнала в папку C:\Trace Folder, выполните команду:*

```
KAVSHELL TRACE /ON /F:"C:\Trace Folder" /LVL:warning
```

Чтобы выключить ведение журнала трассировки, выполните команду:

```
KAVSHELL TRACE /OFF
```

Коды возврата команды KAVSHELL TRACE.

Дефрагментация файлов журналов Kaspersky Embedded Systems Security: KAVSHELL VACUUM

Команда `KAVSHELL VACUUM` позволяет выполнить дефрагментацию файлов журнала программы. Это помогает избежать системных ошибок и ошибок программы из-за хранения большого количества файлов журнала, сформированных на основе событий программы.

Для выполнения команды может потребоваться ввод пароля. Для ввода текущего пароля используйте ключ `[/pwd:<пароль>]`.

Рекомендуется применять команду `KAVSHELL VACUUM` для оптимизации хранения файлов журналов в случае частых запусков задач проверки по требованию и задач обновления. При выполнении команды Kaspersky Embedded Systems Security обновляет логическую структуру файлов журнала программы, хранящихся на защищаемом устройстве по указанному пути.

По умолчанию файлы журнала программы сохраняются в папку C:\ProgramData\Kaspersky Lab\Kaspersky Embedded Systems Security\3.0\Reports. Если вы вручную указали другой путь для хранения файлов журнала, команда `KAVSHELL VACUUM` выполняет дефрагментацию файлов в папке, указанной в параметрах журнала Kaspersky Embedded Systems Security.

Файлы большого размера увеличивают время, необходимое команде `KAVSHELL VACUUM` на выполнение дефрагментации.

Во время выполнения команды `KAVSHELL VACUUM` невозможно выполнение задач постоянной защиты и контроля компьютера. Процедура дефрагментации блокирует доступ к журналу Kaspersky Embedded Systems Security и запрещает запись событий в журнал. Чтобы избежать снижения защиты, рекомендуется планировать запуск команды `KAVSHELL VACUUM`.

Чтобы выполнить дефрагментацию файлов журнала Kaspersky Embedded Systems Security, выполните команду:

```
KAVSHELL VACUUM
```

Для выполнения команды необходимы права учетной записи Локальная система (Local System).

Очищение базы iSwift. KAVSHELL FBRESET

Kaspersky Embedded Systems Security использует технологию iSwift, позволяющую не проверять файл повторно, если с момента последней проверки он не был изменен (**Использовать технологию iSwift**).

Kaspersky Embedded Systems Security создает файлы klamfb.dat и klamfb2.dat в папке %SYSTEMDRIVE%\System Volume Information. Эти файлы содержат информацию о проверенных незараженных объектах. Размер файла klamfb.dat (klamfb2.dat) увеличивается пропорционально количеству файлов, проверенных Kaspersky Embedded Systems Security. В этом файле хранится только актуальная информация о существующих в системе файлах: если файл был удален, то Kaspersky Embedded Systems Security удаляет информацию о нем из файла klamfb.dat.

Для очистки данного файла используйте команду `KAVSHELL FBRESET`.

Учитывайте следующие особенности работы команды `KAVSHELL FBRESET`:

- При очистке файла klamfb.dat с помощью команды KAVSHELL FBRESET, Kaspersky Embedded Systems Security не приостанавливает защиту (в отличие от удаления файла klamfb.dat вручную).
- После очистки файла klamfb.dat Kaspersky Embedded Systems Security может увеличить нагрузку на защищаемое устройство. При этом после очистки файла klamfb.dat Kaspersky Embedded Systems Security проверяет все файлы, к которым обращается впервые. После проверки Kaspersky Embedded Systems Security заново добавляет информацию о каждом проверенном объекте в файл klamfb.dat. При повторном обращении к этому же объекту технология iSwift позволит не проверять файл повторно, если он не был изменен.

Для выполнения команды `KAVSHELL FBRESET` нужно запускать интерпретатор командной строки с правами учетной записи SYSTEM.

Включение и выключение создания файла дампа. KAVSHELL DUMP

Команда `KAVSHELL DUMP` позволяет включать и выключать создание образов памяти (файлов дампов) процессов Kaspersky Embedded Systems Security при их аварийном завершении (см. таблицу ниже). Кроме того, в любой момент можно создать файл дампа для выполняющихся процессов Kaspersky Embedded Systems Security.

Для успешного создания файла дампа, команда `KAVSHELL DUMP` должна быть запущена с правами учетной записи локальной системы (SYSTEM).

Kaspersky Embedded Systems Security записывает информацию в файлы трассировки и файлы дампов в незашифрованном виде.

Синтаксис команды KAVSHELL DUMP

```
KAVSHELL DUMP </ON /F:<папка с файлом дампа>|/SNAPSHOT /F:<папка с файлом дампа> / P:
<pid> | /OFF>
```

Ключ	Описание
/ON	Включить создание файла дампа при аварийном завершении процесса.
/F:<папка с файлами дампов>	Это обязательный параметр. Указывает путь к папке, в которой будет сохранен файл дампа. Нельзя указывать пути к папкам на сетевых дисках других незащищенных устройств. При указании пути к папке с файлом дампа можно использовать системные переменные окружения; пользовательские переменные окружения использовать нельзя.
/SNAPSHOT	Снимает образ памяти выполняющегося процесса с указанным идентификатором и сохраняет файл дампа в папку, указанную параметром /F.
/P	Идентификатор процесса (PID); отображается в Диспетчере задач Microsoft Windows.
/OFF	Выключить создание файла дампа при аварийном завершении процесса.

Коды возврата команды KAVSHELL DUMP.

Примеры команды KAVSHELL DUMP

Чтобы включить создание файла дампа и сохранить файл дампа в папку C:\Dump Folder, выполните команду:

```
KAVSHELL DUMP /ON /F:"C:\Dump Folder"
```

Чтобы снять образ памяти процесса с идентификатором 1234 в папку C:/Dumps, выполните команду:

```
KAVSHELL DUMP /SNAPSHOT /F:C:\dumps /F:1234
```

Чтобы выключить создание файлов дампа, выполните команду:

```
KAVSHELL DUMP /OFF
```

Импорт параметров. KAVSHELL IMPORT

Команда `KAVSHELL IMPORT` позволяет импортировать параметры Kaspersky Embedded Systems Security и текущих задач из конфигурационного файла в Kaspersky Embedded Systems Security на защищаемом устройстве. Вы можете создать конфигурационный файл с помощью команды `KAVSHELL EXPORT`.

Для выполнения команды может потребоваться ввод пароля. Для ввода текущего пароля используйте ключ `[/pwd:<пароль>]`.

Синтаксис команды KAVSHELL IMPORT

```
KAVSHELL IMPORT <имя конфигурационного файла и путь к файлу>
```

Пример команды KAVSHELL IMPORT

```
KAVSHELL IMPORT Host1.xml
```

Параметр команды KAVSHELL IMPORT

Параметр	Описание
<имя конфигурационного файла и путь к файлу>	Имя конфигурационного файла, из которого будут импортированы параметры. Указывая путь к файлу, вы можете использовать системные переменные окружения; вы не можете использовать пользовательские переменные окружения.

Коды возврата команды KAVSHELL IMPORT.

Экспорт параметров. KAVSHELL EXPORT

Команда `KAVSHELL EXPORT` позволяет экспортировать все параметры Kaspersky Embedded Systems Security и его существующих задач в конфигурационный файл, чтобы потом импортировать их в Kaspersky Embedded Systems Security на других защищаемых устройствах.

Синтаксис команды KAVSHELL EXPORT

```
KAVSHELL EXPORT <имя конфигурационного файла и путь к файлу>
```

Пример команды KAVSHELL EXPORT

```
KAVSHELL EXPORT Host1.xml
```

Параметр команды KAVSHELL EXPORT

Параметр	Описание
<имя конфигурационного файла и путь к файлу>	Имя конфигурационного файла, в котором будут сохранены параметры. Конфигурационному файлу можно присвоить любое расширение. Указывая путь к файлу, вы можете использовать системные переменные окружения; вы не можете использовать пользовательские переменные окружения.

Коды возврата команды KAVSHELL EXPORT.

Интеграция с Microsoft Operations Management Suite. KAVSHELL OMSINFO

Команда KAVSHELL OMSINFO позволяет просматривать статус программы и информацию об угрозах, обнаруженных антивирусными базами и службой KSN. Информация об угрозах поступает из доступных журналов событий.

Синтаксис команды KAVSHELL OMSINFO

```
KAVSHELL OMSINFO <полный путь к сформированному файлу с именем файла>
```

Пример команды KAVSHELL OMSINFO

```
KAVSHELL OMSINFO C:\Users\Admin\Desktop\omsinfo.json
```

Параметр команды KAVSHELL OMSINFO

Параметр	Описание
<путь к сформированному файлу с именем файла>	Имя сформированного файла, который будет содержать информацию о статусе программы и обнаруженных угрозах.

Управление задачей Мониторинг целостности файлов на основе эталона: KAVSHELL FIM /BASELINE

Команда `KAVSHELL FIM /BASELINE` позволяет настраивать режим работы задачи Контроль запуска программ и контролировать загрузку DLL-модулей.

Для выполнения команды может потребоваться ввод пароля. Для ввода текущего пароля используйте ключ `[/pwd:<пароль>]`.

Синтаксис команды KAVSHELL FIM /BASELINE

```
KAVSHELL FIM /BASELINE [/CREATE: [<область мониторинга> | /L:<путь к TXT-файлу со списком областей мониторинга>] [/MD5 | /SHA256] [/SF]] | [/CLEAR [/BL:<идентификатор эталона> | /ALIAS:<существующее название>]] | [/EXPORT:<путь к TXT-файлу> [/BL:<идентификатор эталона> | /ALIAS:<существующее название>]] | [/SHOW [/BL:<идентификатор эталона> | /ALIAS:<существующее название>]] | [/SCAN [/BL:<идентификатор эталона> | /ALIAS:<существующее название>]] | [/PWD:<пароль>]
```

Примеры команды KAVSHELL FIM /BASELINE

Чтобы удалить эталон, выполните следующую команду:

```
KAVSHELL FIM /BASELINE /CLEAR /BL:<идентификатор эталона>
```

Вы можете настраивать параметры задачи Контроль запуска программ с помощью ключей (см. таблицу ниже).

Ключи / параметры команды `KAVSHELL FIM/ BASELINE`

Ключ / параметр	Описание
`/CREATE`	Создать задачу Мониторинг целостности файлов на основе эталона. Kaspersky Embedded Systems Security запустит новую задачу Мониторинг целостности файлов на основе эталона, чтобы создать эталон.
`/L`	Укажите путь к TXT-файлу, содержащему список областей мониторинга.
`/MD5`	Укажите алгоритм MD5 для расчета контрольной суммы (необязательный параметр). Параметр `/MD5` не используется совместно с параметром `/SHA256`. Алгоритм MD5 используется по умолчанию.

/SHA256	Укажите алгоритм SHA256 для расчета контрольной суммы (необязательный параметр). Параметр /SHA256 не используется совместно с параметром /MD5. Алгоритм MD5 используется по умолчанию.
/SF	Включить все вложенные папки в область задачи Мониторинг целостности файлов на основе эталона (необязательный параметр). По умолчанию вложенные папки не входят в область задачи Мониторинг целостности файлов на основе эталона.
/CLEAR	Удалить эталон с указанным <идентификатором эталона> или эталон задачи с указанным <существующим названием>. Удалить все эталоны, если не указан ни один из параметров <идентификатор эталона> или <существующее название>. Необязательный параметр.
/BL	Укажите уникальный идентификатор эталона (необязательный параметр).
/EXPORT	Экспортировать данные всех эталонов в TXT-файл.
/SHOW	Показать данные всех эталонов.
/SCAN	Запустить новую задачу Мониторинг целостности файлов на основе эталона с указанным <идентификатором эталона> или <существующим названием>.
/ALIAS	Укажите название новой или существующей задачи.
<область мониторинга>	Укажите файл или папку, которую вы хотите включить в область задачи Мониторинг целостности файлов на основе эталона. Этот параметр позволяет указать только одну область.
<путь к TXT-файлу со списком областей мониторинга>	Укажите путь к TXT-файлу, содержащему список областей мониторинга. Файл должен быть в кодировке UTF-8, а путь к каждой области мониторинга необходимо указывать на отдельной строке.
<путь к TXT-файлу>	Укажите путь к файлу, в который вы хотите экспортировать данные всех эталонов.
<идентификатор эталона>	Укажите уникальный идентификатор эталона. Чтобы просмотреть идентификатор эталона, используйте параметр /SHOW.
<существующее название>	Укажите название существующей задачи.
<новое название>	Укажите название новой задачи.

Коды возврата команд

Коды возврата команд KAVSHELL START и KAVSHELL STOP

Коды возврата команд KAVSHELL START и KAVSHELL STOP

Код	Описание

возврата	
0	Операция выполнена успешно
-3	Ошибка прав доступа
-5	Неверный синтаксис команды
-6	Неверная операция (например, служба Kaspersky Security уже запущена или уже остановлена)
-7	Служба не зарегистрирована
-8	Автоматический запуск службы отключен
-9	Неудачная попытка запустить управляемое устройство под другой учетной записью (по умолчанию служба Kaspersky Security работает под учетной записью Локальная система).
-99	Неизвестная ошибка

Коды возврата команд KAVSHELL SCAN и KAVSHELL SCANCRITICAL

Коды возврата команд KAVSHELL SCAN и KAVSHELL SCANCRITICAL

Код возврата	Описание
0	Операция выполнена успешно (Угроз не обнаружено)
1	Операция отменена
-2	Служба не запущена
-3	Ошибка прав доступа
-4	Объект не найден (не найден файл со списком областей проверки)
-5	Неверный синтаксис команды или не определена область проверки
-80	Зараженных и других обнаруживаемых объектов
-81	Возможно зараженных объектов
-82	Обнаружены ошибки обработки
-83	Обнаружены непроверенные объекты
-84	Обнаружены поврежденные объекты
-85	Не удалось создать журнал выполнения задачи
-99	Неизвестная ошибка
-301	Недействительный ключ

Коды возврата команды KAVSHELL TASK LOG-INSPECTOR

Коды возврата команды KAVSHELL TASK LOG-INSPECTOR

Код возврата	Описание
0	Операция выполнена успешно
-6	Неверная операция (например, служба Kaspersky Security уже запущена или уже

	остановлена)
402	Задача уже запущена (для параметра /STATE)

Коды возврата команды KAVSHELL TASK

Коды возврата команды KAVSHELL TASK

Код возврата	Описание
0	Операция выполнена успешно
-2	Служба не запущена
-3	Ошибка прав доступа
-4	Объект не найден (задача не найдена)
-5	Неверный синтаксис команды
-6	Неверная операция (например, задача не запущена, уже запущена или не может быть приостановлена)
-99	Неизвестная ошибка
-301	Недействительный ключ
401	Задача не запущена (для параметра /STATE)
402	Задача уже запущена (для параметра /STATE)
403	Задача уже приостановлена (для параметра /STATE)
-404	Сбой выполнения операции (изменение состояния задачи привело ее к сбою)

Коды возврата команды KAVSHELL RTP

Коды возврата команды KAVSHELL RTP

Код возврата	Описание
0	Операция выполнена успешно
-2	Служба не запущена
-3	Ошибка прав доступа
-4	Объект не найден (не найдена одна или все задачи постоянной защиты компьютера)
-5	Неверный синтаксис команды
-6	Неверная операция (например, задача уже запущена или уже остановлена)
-99	Неизвестная ошибка
-301	Недействительный ключ

Коды возврата команды KAVSHELL UPDATE

Коды возврата команды KAVSHELL UPDATE

Код возврата	Описание
0	Операция выполнена успешно
200	Все объекты актуальны (базы или программные компоненты в актуальном состоянии)
-2	Служба не запущена
-3	Ошибка прав доступа
-5	Неверный синтаксис команды
-99	Неизвестная ошибка
-206	Файлы обновлений отсутствуют в указанном источнике или имеют неизвестный формат
-209	Ошибка подключения к источнику обновлений
-232	Ошибка аутентификации при подключении к прокси-серверу
-234	Ошибка подключения к программе Kaspersky Security Center
-235	Kaspersky Embedded Systems Security не прошел проверку подлинности при соединении с источником обновлений
-236	Базы программы повреждены
-301	Недействительный ключ

Коды возврата команды KAVSHELL ROLLBACK

Коды возврата команды KAVSHELL ROLLBACK

Код возврата	Описание
0	Операция выполнена успешно
-2	Служба не запущена
-3	Ошибка прав доступа
-99	Неизвестная ошибка
-221	Резервная копия баз не найдена
-222	Резервная копия баз повреждена

Коды возврата команды KAVSHELL LICENSE

Коды возврата команды KAVSHELL LICENSE

Код возврата	Описание
0	Операция выполнена успешно
-2	Служба не запущена
-3	Недостаточно прав для управления ключами
-4	Ключ с указанным номером не найден
-5	Неверный синтаксис команды

-6	Неверная операция (ключ уже добавлен)
-99	Неизвестная ошибка
-301	Недействительный ключ
-303	Лицензия распространяется на другую программу

Коды возврата команды KAVSHELL TRACE

Коды возврата команды KAVSHELL TRACE

Код возврата	Описание
0	Операция выполнена успешно
-2	Служба не запущена
-3	Ошибка прав доступа
-4	Объект не найден (не найден путь к папке с файлами журнала трассировки)
-5	Неверный синтаксис команды
-6	Недопустимая операция (попытка выполнения команды KAVSHELL TRACE /OFF, если создание журнала трассировки уже выключено)
-99	Неизвестная ошибка

Коды возврата команды KAVSHELL FBRESET

Коды возврата команды KAVSHELL FBRESET

Код возврата	Описание
0	Операция выполнена успешно
-99	Неизвестная ошибка

Коды возврата команды KAVSHELL DUMP

Коды возврата команды KAVSHELL DUMP

Код возврата	Описание
0	Операция выполнена успешно
-2	Служба не запущена
-3	Ошибка прав доступа
-4	Объект не найден (не найден путь к папке с файлом дампа; не найден процесс с указанным идентификатором)
-5	Неверный синтаксис команды
-6	Неверная операция (попытка выполнения команды KAVSHELL DUMP /OFF, если создание

	файла дампа уже выключено)
-99	Неизвестная ошибка

Коды возврата команды KAVSHELL IMPORT

Коды возврата команды KAVSHELL IMPORT

Код возврата	Описание
0	Операция выполнена успешно
-2	Служба не запущена
-3	Ошибка прав доступа
-4	Объект не найден (не удается найти конфигурационный файл для импорта)
-5	Неверный синтаксис
-99	Неизвестная ошибка
501	Операция выполнена успешно, однако во время выполнения возникла ошибка / замечание (например, программа Kaspersky Embedded Systems Security не импортировала параметры некоторых функциональных компонентов)
-502	Файл импорта отсутствует или имеет неизвестный формат
-503	Несовместимые параметры (конфигурационный файл экспортирован из другой программы или Kaspersky Embedded Systems Security более поздней или несовместимой версии)

Коды возврата команды KAVSHELL EXPORT

Коды возврата команды KAVSHELL EXPORT

Код возврата	Описание
0	Операция выполнена успешно
-2	Служба не запущена
-3	Ошибка прав доступа
-5	Неверный синтаксис
-10	Не удалось создать конфигурационный файл (например, нет доступа к папке, указанной в пути к файлу)
-99	Неизвестная ошибка
501	Операция выполнена успешно, однако во время выполнения возникла ошибка / замечание (например, программа Kaspersky Embedded Systems Security не экспортировала параметры некоторых функциональных компонентов)

Коды возврата команды KAVSHELL FIM /BASELINE

Коды возврата команды KAVSHELL FIM /BASELINE

Код возврата	Описание
0	Операция выполнена успешно
-2	Служба не запущена
-3	Ошибка прав доступа
-4	Объект не найден (задача не найдена)
-5	Неверный синтаксис команды
-6	Неверная операция (например, эталон был удален)
-10	Не удалось создать конфигурационный файл (например, нет доступа к папке, указанной в пути к файлу)
-12	Неверный пароль
-80	Не соответствует удаленным эталонным объектам
-85	Не удалось создать журнал выполнения задачи
-99	Внутренняя ошибка
-303	Недопустимый лицензионный ключ
-502	Задача не запущена
200	Все объекты соответствуют эталону
501	Задача завершена успешно с ошибкой / комментарием

Обращение в Службу технической поддержки

Этот раздел содержит информацию о способах и условиях получения технической поддержки.

Способы получения технической поддержки

Если вы не нашли решения вашей проблемы в документации или других источниках информации о программе, рекомендуется обратиться в Службу технической поддержки. Сотрудники Службы технической поддержки ответят на ваши вопросы об установке и использовании программы.

Техническая поддержка предоставляется только пользователям, которые приобрели коммерческую лицензию на использование программы. Пользователям, которые получили пробную лицензию, техническая поддержка не предоставляется.

Перед обращением в Службу технической поддержки ознакомьтесь с правилами предоставления технической поддержки.

Вы можете связаться со специалистами Службы технической поддержки одним из следующих способов:

- Позвонить в Службу технической поддержки по телефону.
- Отправить запрос в Службу технической поддержки "Лаборатории Касперского" с портала Kaspersky CompanyAccount.

Получение технической поддержки по телефону

В большинстве регионов по всему миру вы можете позвонить специалистам Службы технической поддержки. Вы можете найти информацию о способах получения технической поддержки в вашем регионе и контакты Службы технической поддержки на веб-сайте Службы технической поддержки "Лаборатории Касперского".

Перед обращением в Службу технической поддержки ознакомьтесь с правилами предоставления технической поддержки.

Техническая поддержка через Kaspersky CompanyAccount

Kaspersky CompanyAccount – это портал для организаций, использующих программы "Лаборатории Касперского". Портал Kaspersky CompanyAccount предназначен для взаимодействия пользователей со специалистами "Лаборатории Касперского" с помощью электронных запросов. На портале Kaspersky CompanyAccount можно отслеживать статус обработки электронных запросов специалистами "Лаборатории Касперского" и хранить историю электронных запросов.

Вы можете зарегистрировать всех сотрудников вашей организации в рамках одной учетной записи Kaspersky CompanyAccount. Одна учетная запись позволяет вам централизованно управлять электронными запросами от зарегистрированных сотрудников в "Лабораторию Касперского", а также управлять правами этих сотрудников в Kaspersky CompanyAccount.

Портал Kaspersky CompanyAccount доступен на следующих языках:

- английском;
- испанском;
- итальянском;
- немецком;
- польском;
- португальском;
- русском;
- французском;
- японском.

Дополнительная информация о Kaspersky CompanyAccount приведена на веб-сайте Службы технической поддержки.

Использование файла трассировки и скрипта AVZ

После того как вы сообщите специалистам Службы технической поддержки "Лаборатории Касперского" о возникшей проблеме, вас могут попросить сформировать отчет с информацией о работе Kaspersky Embedded Systems Security и отправить его в Службу технической поддержки "Лаборатории Касперского". Также специалисты Службы технической поддержки "Лаборатории Касперского" могут попросить вас создать файл трассировки. Файл трассировки позволяет отследить процесс пошагового выполнения команд программы и обнаружить, на каком этапе работы программы возникает ошибка.

В результате анализа присланных вами данных специалисты Службы технической поддержки "Лаборатории Касперского" могут создать и отправить вам скрипт AVZ. Выполнение скриптов AVZ позволяет проводить анализ запущенных процессов на наличие угроз, проверять защищаемое устройство на наличие угроз, лечить или удалять зараженные файлы и создавать отчеты о результатах проверки системы.

Для более эффективного оказания поддержки в случае возникновения вопросов по работе программы специалисты Службы технической поддержки могут попросить вас в отладочных целях на время проведения работ по диагностике изменить параметры программы. Для этого может потребоваться выполнение следующих действий:

- Активировать функциональность обработки и сохранения расширенной диагностической информации.
- Выполнить более тонкую настройку работы отдельных компонентов программы, недоступную через стандартные средства пользовательского интерфейса.
- Изменить параметры хранения и отправки сохраняемой диагностической информации.
- Настроить перехват и сохранение в файл сетевого трафика.

Глоссарий

Kaspersky Security Network (KSN)

Инфраструктура облачных служб, предоставляющая доступ к оперативной базе данных "Лаборатории Касперского" с постоянно обновляемой информацией о репутации файлов, веб-ресурсов и программ. Kaspersky Security Network обеспечивает более высокую скорость реакции программ "Лаборатории Касперского" на угрозы, повышает эффективность работы некоторых компонентов защиты, а также снижает вероятность ложных срабатываний.

OLE-объект

Объект, прикрепленный к другому файлу или вложенный в другой файл путем использования технологии Object Linking and Embedding (OLE). Например, OLE-объектом является таблица Microsoft Office Excel®, встроенная в документ Microsoft Office Word.

SIEM

Технология, которая обеспечивает анализ событий безопасности, исходящих от различных сетевых устройств и приложений.

Активный ключ

Ключ, используемый в текущий момент для работы программы.

Антивирусные базы

Базы данных, которые содержат информацию об угрозах компьютерной безопасности, известных "Лаборатории Касперского" на момент выпуска антивирусных баз. Записи в антивирусных базах позволяют обнаруживать вредоносный код в проверяемых объектах. Антивирусные базы создаются специалистами "Лаборатории Касперского" и обновляются каждый час.

Архив

Один или несколько файлов, упакованных в один файл в сжатом виде. Для архивирования и разархивирования данных требуется специальная программа – архиватор.

Задача

Функции, выполняемые программой "Лаборатории Касперского", реализованы в виде задач, например: Постоянная защита файлов, Полная проверка компьютера и Обновление баз программы.

Зараженный объект

Объект, часть кода которого полностью совпадает с частью кода известной вредоносной программы. "Лаборатория Касперского" не рекомендует обрабатывать такие объекты.

Карантин

Папка, в которую программа "Лаборатории Касперского" перемещает обнаруженные возможно зараженные объекты. Объекты на карантине хранятся в зашифрованном виде во избежание их воздействия на компьютер.

Лечение объектов

Способ обработки зараженных объектов, в результате применения которого происходит полное или частичное восстановление данных. Не все зараженные объекты можно вылечить.

Ложное срабатывание

Ситуация, когда незараженный объект определяется программой "Лаборатории Касперского" как зараженный из-за того, что его код напоминает код вируса.

Локальная задача

Задача, определенная и работающая на отдельном клиентском компьютере.

Маска файла

Представление имени файла с помощью специальных символов. Стандартными специальными символами, используемыми в масках файлов, являются * и ?, где * представляет любое количество символов, а ? представляет любой отдельный символ.

Обновление

Процедура замены/добавления новых файлов (баз или программных модулей), получаемых с серверов обновлений "Лаборатории Касперского".

Объекты автозапуска

Набор программ, необходимых для запуска и корректной работы установленных на вашем компьютере операционной системы и программного обеспечения. Каждый раз при старте операционная система запускает эти объекты. Существуют вирусы, способные поражать именно такие объекты, что может привести, например, к блокированию запуска операционной системы.

Параметры задачи

Параметры программы, специфические для каждого типа задач.

Политика

Политика определяет параметры работы программы и доступ к настройке программы, установленной на компьютерах одной группы администрирования. Для каждой программы требуется создать свою политику. Вы можете создать неограниченное количество различных политик для программ, установленных на компьютерах в каждой группе администрирования, но в пределах группы администрирования только одна политика может применяться единовременно к каждой программе.

Потенциально заражаемый файл

Файл, который в силу своей структуры или формата может быть использован злоумышленниками в качестве "контейнера" для размещения и распространения вредоносного кода. Как правило, это исполняемые файлы, например, с расширением com, exe и dll. Риск проникновения вредоносного кода в такие файлы весьма высок.

Резервное хранилище

Специальное хранилище для резервных копий файлов, которые создаются перед попыткой дезинфекции или удаления.

Сервер администрирования

Компонент программы Kaspersky Security Center, осуществляющий функции централизованного хранения информации об установленных в сети организации программах "Лаборатории Касперского". Его также можно использовать для управления этими программами.

Срок действия лицензии

Период, в течение которого у вас есть доступ к функциям программы и право использовать дополнительные службы. Службы, которые вы можете использовать, зависят от типа лицензии.

Статус защиты

Текущий статус защиты, характеризующий степень защищенности компьютера.

Уровень безопасности

Уровень безопасности представляет собой предварительно заданный набор параметров компонентов программы.

Уровень важности события

Характеристика события, зафиксированного в работе программы "Лаборатории Касперского". Существуют следующие уровни важности:

- Критическое событие
- Отказ функционирования
- Предупреждение
- Информационное сообщение

События одного и того же типа могут иметь различные уровни важности, в зависимости от ситуации, при которой событие произошло.

Уязвимость

Недостаток в операционной системе или программе, который может быть использован производителями вредоносного программного обеспечения для проникновения в операционную систему или программу и нарушения ее целостности. Большое количество уязвимостей в операционной системе делает ее работу ненадежной, так как внедрившиеся в операционную систему вирусы могут вызывать сбои в работе как самой операционной системы, так и установленных программ.

Эвристический анализатор

Технология обнаружения угроз, информация о которых еще не занесена в базы "Лаборатории Касперского". Эвристический анализатор позволяет обнаруживать объекты, поведение которых в операционной системе может представлять угрозу безопасности. Объекты, обнаруженные с помощью эвристического анализатора, признаются возможно зараженными. Например, возможно зараженным может быть признан объект, который содержит последовательности команд, свойственные вредоносным объектам (открытие файла, запись в файл).

Информация о стороннем коде

Информация о стороннем коде содержится в файле legal_notices.txt, расположенном в папке установки программы.

Уведомления о товарных знаках

Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.

Intel и Pentium – товарные знаки Intel Corporation, зарегистрированные в Соединенных Штатах Америки и в других странах.

Linux – товарный знак Linus Torvalds, зарегистрированный в США и в других странах.

Microsoft, Active Directory, Excel, Internet Explorer, Outlook, Windows и Windows Server – товарные знаки Microsoft Corporation, зарегистрированные в Соединенных Штатах Америки и в других странах.

UNIX – товарный знак, зарегистрированный в США и других странах, использование лицензировано X/Open Company Limited.